DOSSIER DE DEMANDE D'AUTORISATION ENVIRONNEMENTALE AU TITRE DES INSTALLATIONS CLASSÉES (ICPE)

PROJET DE PLATEFORME DE LOGISTIQUE URBAINE MULTIMODALE SUR LE PORT DE GENNEVILLIERS (92)

PROJET GREEN DOCK

PARTIE 6

Pièce 6.5b
Annexes de l'ESSP

Cahier 5/5

Sommaire

Le 26 décembre 2016

Décret n°2000-376 du 28 avril 2000 relatif à la protection des transports de fonds

NOR: INTD0000109D

Version consolidée au 30 novembre 2014

Le Premier ministre,

Sur le rapport du garde des sceaux, ministre de la justice, et du ministre de l'intérieur,

Vu le code pénal ;

Vu le code des postes et télécommunications, notamment ses articles D. 51 et D. 52 ;

Vu la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de surveillance, de gardiennage et de transport de fonds ;

Vu le décret du 18 avril 1939 modifié fixant le régime des matériels de guerre, armes et munitions ;

Vu le décret n° 86-1058 du 28 septembre 1986 relatif à l'autorisation administrative et au recrutement des personnels des entreprises de surveillance et de gardiennage, de transport de fonds et de protection de personnes ;

Vu le décret n° 86-1099 du 10 octobre 1986 relatif à l'utilisation des matériels, documents, uniformes et insignes des entreprises de surveillance et de gardiennage, transport de fonds et protection de personnes ;

Vu le décret n° 95-589 du 6 mai 1995 modifié relatif à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Article 1 (abrogé au 1 décembre 2014)

· Modifié par Décret n°2013-959 du 25 octobre 2013 - art. 1
· Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I. - Sont soumis aux dispositions du présent décret tous les transports sur la voie publique :

1° De fonds ou de métaux précieux représentant une valeur d'au moins 30 000 euros ;

2° De bijoux, représentant une valeur d'au moins 100 000 euros.

Lorsque, pour le transport de monnaie fiduciaire, le montant total des fonds transportés, dans le cadre d'une ou plusieurs prestations d'un même circuit au départ d'un lieu sécurisé, est inférieur à 30 000 euros, et que le donneur d'ordres fait appel à une entreprise de transport de fonds, le transport s'effectue dans un véhicule banalisé, dans les conditions prévues à l'article 8. En ce cas, l'équipage, non armé, peut n'être composé que d'une personne.

Les fonds sont placés dans des dispositifs garantissant qu'ils pourront être rendus impropres à leur destination et qui soit sont en nombre au moins égal à celui des points de desserte, soit sont équipés d'un système de collecteur ne pouvant être ouvert que dans une zone ou un lieu sécurisés. (1)

La valeur des fonds, métaux précieux et bijoux mentionnés ci-dessus est celle déclarée au transporteur de fonds.

II. - Sont considérés comme fonds au titre du présent décret la monnaie fiduciaire, la monnaie divisionnaire et le papier fiduciaire destiné à l'impression des billets. Tout transport de papier fiduciaire est regardé comme représentant une valeur d'au moins 30 000 euros.

III. - Sont considérés comme bijoux au titre du présent décret les objets, y compris d'horlogerie, destinés à la parure qui comprennent des métaux précieux soumis aux titres légaux, des matériaux rares ou issus de technologies innovantes, des pierres précieuses ou des perles fines ou de culture ainsi que les éléments de bijouterie en métal précieux entrant dans le cycle de fabrication.

IV. - Ne sont pas soumis aux dispositions du présent décret :

1° Les transports mentionnés au I :

a) Effectués par une personne physique pour son propre compte ou par les dirigeants ou gérants d'une personne morale pour le compte de celle-ci ;

b) Effectués par l'autorité militaire ;

c) Ou dont la protection est assurée par une escorte de la gendarmerie nationale ou de la police nationale ;

2° Les transports :

a) Des timbres-poste non oblitérés ;

b) Des lettres et des paquets chargés dans les conditions prévues aux articles D. 51 et D. 52 du code des postes et communications électroniques.

NOTA :
(1) Conformément à l'article 5 du décret n° 2013-959 du 25 octobre 2013, les dispositions du cinquième alinéa de l'article 1er du décret du 28 avril 2000, dans leur rédaction issue du présent décret, entrent en vigueur le 1er juillet 2014.

Article 1-1 (abrogé au 1 décembre 2014)

- Créé par Décret n°2012-1109 du 1er octobre 2012 - art. 2
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Au sens du présent décret, on entend par :
1° Zone sécurisée : un point de dépôt, de collecte ou de traitement des fonds dans un espace, séparé et fermé, d'un bâtiment, dans lequel les fonds, bijoux ou métaux précieux peuvent être introduits, retirés ou manipulés de manière sûre ; pour l'application des articles 2 et 8-1, un véhicule blindé répondant aux conditions de l'article 4 est assimilé à une zone sécurisée ;
2° Lieu sécurisé : un espace, au sein d'un bâtiment, dans lequel un véhicule de transport de fonds a accès et est chargé ou déchargé de manière sûre ;
3° Automates bancaires : les distributeurs automatiques de billets et les guichets automatiques de banque ;
4° Entreprise de transport de fonds : une personne physique ou morale exerçant l'activité de transport de fonds, de bijoux ou de métaux précieux définie au 2° de l'article L. 611-1 du code de la sécurité intérieure ;
5° Véhicule de transport de fonds : un véhicule, équipé ou non de blindages, utilisé pour le transport professionnel des fonds, bijoux ou métaux précieux.
Ne peut être utilisé comme véhicule de transport de fonds qu'un véhicule comportant au minimum quatre roues.

Article 2 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2013-959 du 25 octobre 2013 - art. 2
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I. - La monnaie fiduciaire et le papier fiduciaire destiné à l'impression des billets sont transportés :

1° Soit dans des véhicules blindés, avec un équipage d'au moins trois personnes y compris le conducteur, conformes aux dispositions de l'article 4 ;

2° Soit dans des véhicules blindés, conformes aux dispositions de l'article 4 et équipés de dispositifs garantissant que les fonds transportés pourront être rendus impropres à leur destination, dans les conditions prévues à l'article 8-1.

Si ces véhicules sont équipés d'au moins autant de dispositifs mentionnés à l'alinéa précédent que de points de desserte, leur équipage est d'au moins deux personnes y compris le conducteur. Les dispositions du II de l'article 4 peuvent, dans cette hypothèse, ne s'appliquer qu'à la cabine de conduite du véhicule.

Si ces véhicules sont équipés de moins de dispositifs mentionnés au premier alinéa que de points de desserte, leur équipage est d'au moins trois personnes y compris le conducteur.

3° Soit dans des véhicules banalisés, avec un équipage d'au moins deux personnes y compris le conducteur, dans les conditions prévues aux articles 7 et 8, dès lors que les fonds sont placés dans des dispositifs garantissant qu'ils pourront être rendus impropres à leur destination et que ces dispositifs soit sont en nombre au moins égal à celui des points de desserte, soit sont équipés d'un système de collecteur qui ne peut être ouvert que dans une zone ou un lieu sécurisés.

Toutefois, pour la desserte des automates bancaires situés dans certaines zones à risques, les fonds sont obligatoirement transportés dans les conditions prévues au 1° et les automates rechargés par l'un des membres de l'équipage. La liste de ces zones, révisable annuellement, est établie par convention nationale conclue entre l'Etat et les organisations les plus représentatives des établissements de crédit et des établissements financiers, d'une part, et des transporteurs de fonds, d'autre part. A défaut de convention dans un délai de six mois à compter de la publication du décret n° 2012-1109 du 1er octobre 2012 ou de révision de la convention plus de dix-huit mois à compter de sa conclusion ou de sa dernière modification, la liste peut être fixée ou modifiée par arrêté du ministre de l'intérieur. Ce dispositif ne s'applique que lorsque le stationnement du véhicule blindé de transport de fonds en protection de l'immeuble ou de l'automate bancaire est possible. Il entre en vigueur dans les conditions prévues par la convention ou l'arrêté et, au plus tard, dans un délai de douze mois à compter de leur signature.

II. - Les bijoux et les métaux précieux doivent être transportés :

1° Soit dans des véhicules blindés dans les conditions prévues au 1° du I du présent article ;

2° Soit avec un équipage d'au moins deux personnes y compris le conducteur dans des véhicules banalisés dans les conditions prévues à l'article 7 et aux quatre premiers alinéas de l'article 8.

III. - La monnaie divisionnaire et l'or d'investissement au sens de l'article 298 sexdecies A du code général des impôts sont transportés dans des véhicules blindés, avec un équipage d'au moins trois personnes y compris le conducteur, conformes aux dispositions de l'article 4.

Toutefois, pour l'application du règlement n° 1214/2011 du Parlement européen et du Conseil du 16 novembre 2011, les entreprises titulaires d'une licence de transport de fonds transfrontalier délivrée par le Conseil national des activités privées de sécurité peuvent assurer le transport de monnaie divisionnaire soit au moyen d'un véhicule blindé, dans les conditions prévues à l'alinéa précédent, soit au moyen d'un véhicule semi-blindé transportant uniquement des pièces, dans les conditions prévues à l'article 4 du présent décret. Le véhicule semi-blindé est muni d'un marquage très visible indiquant qu'il ne transporte que des pièces et correspondant au pictogramme représenté à l'annexe IV du règlement européen susvisé.

Par dérogation au premier alinéa du présent III, pour les transports de la Banque de France comprenant au maximum 115 000 euros en pièces de 1 ou 2 euros, la monnaie

divisionnaire est transportée :

1° Dans des véhicules blindés sur lesquels ne figure pas la raison sociale de l'entreprise de transport de fonds, avec un équipage d'au moins deux personnes armées et en tenue, y compris le conducteur, dans les conditions prévues aux trois premiers alinéas de l'article 8 ;

2° Ou, si le volume total transporté n'excède pas 500 000 euros et si les points d'arrêts relevant de la Banque de France, des entreprises de transport de fonds, de la gendarmerie ou de la police nationales sont des lieux sécurisés, dans des véhicules semi-blindés sur lesquels ne figure pas la raison sociale de l'entreprise de transport de fonds, avec un équipage d'au moins deux personnes armées et en tenue, y compris le conducteur, dans les conditions prévues aux trois premiers alinéas de l'article 8.

Article 2-1 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2013-959 du 25 octobre 2013 - art. 3
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I. — Les circuits des véhicules de transport de fonds sont préparés par les entreprises de transport de fonds de façon à assurer le départ d'un lieu sécurisé et la variation des itinéraires. Pour les transports desservant les succursales de la Banque de France, une convention conclue entre celle-ci et l'entreprise de transport de fonds précise cette obligation.

II. — Un circuit peut comprendre plusieurs points de desserte.

Le temps d'arrêt ne peut excéder quinze minutes par automate bancaire desservi. Lorsque plusieurs automates bancaires sont desservis et pour toute autre desserte, il ne peut excéder trente minutes au total.

Le nombre d'allers-retours d'un convoyeur de fonds entre le véhicule de transport de fonds et le point de desserte est limité à trois. Lors de chaque aller-retour, les fonds sont placés dans des dispositifs garantissant qu'ils pourront être rendus impropres à leur destination, dans les conditions prévues à l'article 8-1 du présent décret.

Lorsque les circonstances particulières rendent impossible la limitation à trois allers-retours entre le véhicule blindé et le point de dépôt ou de collecte de monnaie métallique, une dérogation peut être accordée par le préfet sur avis de la commission départementale de la sécurité des transports de fonds.

En cas de transport par véhicule blindé, le convoyeur de fonds assurant le rôle de garde ne participe pas au portage de fonds entre le véhicule et le point de desserte. Le convoyeur assurant le rôle de messager doit, à tout moment, conserver une main libre.

III. — Un convoyeur de fonds ne peut avoir accès à un lieu sécurisé ou à une zone sécurisée qu'après identification, par tout moyen, par le gestionnaire du point d'arrêt.

Article 3 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2013-723 du 12 août 2013 - art. 6
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Sauf pour les transports auxquels l'article 7 s'applique, chacun des convoyeurs faisant partie de l'équipage d'un véhicule de transport de fonds porte une arme du 1° de la catégorie B de l'article 2 du décret n° 2013-700 du 30 juillet 2013 portant application de la loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes moderne, simplifié et préventif, ainsi que les munitions correspondantes classées au 10° de la catégorie B.
Tout véhicule blindé est en outre équipé d'une arme complémentaire du f du 2° de la catégorie B de l'article 2 du décret du 30 juillet 2013, ainsi que des munitions correspondantes classées au 8° de la catégorie C.

Article 4 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 6
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I. - Le véhicule équipé de blindages est aménagé de manière à assurer la sécurité du personnel ainsi que celle des fonds, bijoux ou métaux précieux transportés.
Il est équipé au moins :
1° D'un système de communication et d'un système d'alarme, reliés au centre d'alerte de l'entreprise chargée du transport de fonds ;
2° D'un système de repérage à distance permettant à l'entreprise d'en déterminer à tout moment l'emplacement ;
3° De gilets pare-balles et de masques à gaz, en nombre au moins égal à celui des membres de l'équipage et, éventuellement, des personnes ayant une raison légitime de se trouver dans le véhicule.
II. - Les types de véhicule, les modèles de blindage des parois et de vitrage, ainsi que les caractéristiques des autres éléments concourant à la sécurité des véhicules équipés de blindages, sont soumis à l'agrément préalable du ministre de l'intérieur, sur la base des normes minimales, notamment de résistance, que celui-ci définit par un arrêté qui fixe également la composition du dossier de demande d'agrément.
Aux fins d'agrément des véhicules de transport de fonds équipés de blindages importés des autres Etats membres de l'Union européenne ou parties à l'accord sur l'Espace économique européen, sont acceptés les rapports d'essais et les certificats établis par un organisme agréé ou accrédité dans ces Etats qui attestent la conformité de ces blindages à des conditions techniques et réglementaires assurant un niveau de protection équivalent à celui prévu par le présent décret et l'arrêté mentionné à l'alinéa précédent.
Toute modification substantielle des conditions de fabrication des véhicules ou des conditions de fabrication ou d'installation des blindages, vitrages et autres éléments mentionnés à l'alinéa précédent donne lieu à un nouvel agrément.
L'agrément peut être retiré si les matériels mentionnés au II du présent article ne permettent plus d'assurer la sécurité du personnel ou celle des fonds transportés.

Article 5 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 7
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Lorsqu'il n'est pas en service, y compris en raison de travaux d'entretien ou de réparation, le véhicule de transport de fonds équipé de blindages est garé dans un local auquel ne peuvent avoir accès que le conducteur et le personnel chargé de l'entretien ou des réparations.
Avant toute cession d'un véhicule de transport de fonds équipé de blindages, même en vue de sa destruction, ou toute utilisation d'un tel véhicule pour un usage autre que celui prévu par le présent décret, l'entreprise de transport de fonds s'assure de l'agrément du

préfet du département dans lequel se situe son siège, qui se prononce au regard des risques que la cession ou l'utilisation peut présenter pour la sécurité publique.

Article 6 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 8
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Durant l'exécution de la mission en véhicule de transport de fonds, sauf si l'article 7 s'applique, chaque convoyeur est revêtu d'une tenue qui ne doit pas prêter à confusion avec les uniformes définis par des textes législatifs ou réglementaires.

Le port du gilet pare-balles, dont le modèle est fixé par un arrêté du ministre de l'intérieur et du ministre chargé des transports, est obligatoire pour tout convoyeur que l'exécution de la mission conduit à sortir du véhicule.

Durant l'exécution de la mission, les armes de poing sont portées dans leur étui ; l'arme complémentaire mentionnée au deuxième alinéa de l'article 3 ne doit pas quitter le véhicule. Suivant leur type, les armes sont en position de sécurité ou non armées.

Les armes ne peuvent être utilisées qu'en cas de légitime défense, dans les conditions prévues à l'article 122-5 du code pénal.

Article 7 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2004-295 du 29 mars 2004 - art. 3 JORF 30 mars 2004
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

L'équipage d'un véhicule banalisé servant au transport de billets, de bijoux ou de métaux précieux n'est pas armé et n'est pas soumis aux dispositions de l'article 1er du décret du 10 octobre 1986 susvisé.

Article 8 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 9
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Tout véhicule banalisé servant au transport de fonds placés dans les dispositifs mentionnés au 3° du I de l'article 2 ou servant au transport de bijoux ou de métaux précieux est équipé au moins :.

1° D'un système de communication et d'un système d'alarme, reliés au centre d'alerte de l'entreprise chargée du transport de fonds ;

2° D'un système de repérage à distance permettant à l'entreprise d'en déterminer à tout moment l'emplacement.

Un véhicule banalisé n'est pas nécessairement équipé de blindages. L'entreprise de transport de fonds n'est pas astreinte à y faire figurer sa raison sociale.

Article 8-1 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2013-959 du 25 octobre 2013 - art. 4
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I. - Aucun dispositif garantissant que les fonds transportés pourront être rendus impropres à leur destination ne peut être mis en oeuvre sans un agrément délivré, pour une période de cinq ans, par le ministre de l'intérieur après avis de la commission technique prévue à l'article 9. Cet agrément porte sur les caractéristiques techniques et les conditions d'utilisation de ces dispositifs. Il est subordonné à la réussite de divers tests dans un laboratoire d'essais reconnu par arrêté du ministre de l'intérieur.

Lors de la demande d'agrément, le demandeur fournit à la commission un échantillon de la substance utilisée pour assurer la neutralisation et la traçabilité des billets. Les informations sur la composition de cette substance sont transmises aux laboratoires de la police et de la gendarmerie nationales chargés d'analyser les billets maculés après toute attaque ou agression, ou leur sont accessibles.

La commission peut, si elle l'estime nécessaire, inviter le demandeur à faire procéder à des essais complémentaires ou procéder à toute investigation supplémentaire. Ces essais ou ces investigations sont à la charge du demandeur.

Toute modification substantielle des dispositifs ou de leurs caractéristiques techniques donne lieu à un nouvel agrément.

Toute modification substantielle des caractéristiques des billets utilisés lors des tests nécessite un nouvel agrément de ce dispositif pour le transport de ce type de billets.

Chaque type de sac utilisable par un dispositif doit avoir été vérifié avec les mêmes protocoles de tests et obtenir l'agrément dans les mêmes conditions.

II. - Un dispositif de neutralisation de billets répond aux conditions suivantes :

1° Le conteneur, réceptacle dans lequel sont placés les billets transportés, contient soit des billets, avec ou sans sacs, soit une ou plusieurs cassettes pour automate bancaire ou pour d'autres types de distributeur ;

2° Le conteneur assure la protection ininterrompue des billets au moyen d'un mécanisme de neutralisation, depuis une zone sécurisée jusqu'au point de livraison ou depuis le point de collecte jusqu'à une zone sécurisée ;

3° Le conteneur ne peut être programmé que dans une zone sécurisée ou un lieu sécurisé ;

4° Dès lors que le transport a débuté, les convoyeurs de fonds ne peuvent ouvrir le conteneur en dehors des zones ou des lieux sécurisés, ni modifier les plages horaires ni les zones sécurisées où le conteneur peut être ouvert. Ils peuvent cependant, si le dispositif est équipé d'une temporisation, le faire fonctionner une fois, en cas de nécessité de prolonger pour un trajet le temps passé à l'extérieur du véhicule en dehors d'un lieu ou d'une zone sécurisé ; en outre, une possibilité d'ouverture du conteneur en dehors des

conditions d'accès programmée peut être prévue en cas de transport dans un véhicule blindé conforme aux dispositions de l'article 4, dans l'hypothèse où le nombre de conteneurs transportés est inférieur au nombre de points de desserte ;

5° Le conteneur est équipé d'un mécanisme qui neutralise la totalité des billets de façon immédiate et définitive en cas de tentative d'ouverture non autorisée ;

6° La neutralisation affecte au moins 20 % de chaque face de chacun des billets de banque, ensachés ou non ; elle est irréversible et reconnaissable de façon évidente par les utilisateurs ;

7° Les substances ou éléments utilisés pour assurer la neutralisation des billets contiennent un ou plusieurs éléments traceurs permettant de caractériser de façon unique leur origine et le conteneur dans lequel ils étaient placés.

III. - Un arrêté du ministre de l'intérieur fixe :

1° Les caractéristiques techniques auxquelles satisfont les dispositifs de neutralisation de billets, notamment les informations qu'enregistre le système de programmation du conteneur, les informations qui font l'objet d'une authentification, les caractéristiques des substances ou éléments utilisés pour assurer la neutralisation des billets et celles des éléments traceurs qu'ils contiennent ;

2° La nature des tests de résistance à la fraude et de neutralisation auxquels les dispositifs sont soumis ;

3° La composition du dossier de demande d'agrément ;

4° Le modèle du pictogramme d'information figurant sur les dispositifs agréés.

IV. - Aux fins d'agrément des dispositifs de neutralisation importés des autres Etats membres de l'Union européenne ou parties à l'accord sur l'Espace économique européen, sont acceptés les rapports d'essais et les certificats établis par un organisme agréé ou accrédité dans ces Etats qui attestent la conformité de ces dispositifs à des conditions techniques et réglementaires assurant un niveau de protection équivalent à celui prévu par le présent décret et l'arrêté mentionné au III.

IV. - Une entreprise de transport de fonds peut utiliser un dispositif de neutralisation de billets à condition de respecter le fonctionnement et les préconisations du constructeur en matière de maintenance tels que décrits dans l'agrément.

VI. - Le dispositif de neutralisation, dont l'agrément a été délivré antérieurement au 1er décembre 2012 mais est venu à expiration, peut toutefois continuer à être utilisé pendant une durée maximale de quatre années après sa date d'acquisition, dès lors que cette date est antérieure à la date d'expiration de l'agrément.

Article 8-2 (abrogé au 1 décembre 2014)

- Créé par Décret n°2012-1109 du 1er octobre 2012 - art. 11
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16
- I. — Les dispositifs garantissant que les fonds délivrés ou déposés dans un automate

bancaire pourront être rendus impropres à leur destination sont soumis à un agrément délivré, pour une période de cinq ans, par le ministre de l'intérieur après avis de la commission technique prévue à l'article 9. Cet agrément porte sur les caractéristiques techniques et les conditions d'utilisation de ces dispositifs. Il est subordonné à la réussite de divers tests dans un laboratoire d'essais reconnu par arrêté du ministre de l'intérieur.

Lors de la demande d'agrément, le demandeur fournit à la commission un échantillon de la substance utilisée pour assurer la neutralisation et la traçabilité des billets. Les informations sur la composition de cette substance sont transmises aux laboratoires de la police et de la gendarmerie nationales chargés d'analyser les billets maculés après toute attaque ou agression, ou leur sont accessibles.

La commission peut, si elle l'estime nécessaire, inviter le demandeur à faire procéder à des essais complémentaires ou procéder à toute investigation supplémentaire. Ces essais ou ces investigations sont à la charge du demandeur.

Toute modification substantielle des dispositifs ou de leurs caractéristiques techniques ou des caractéristiques des billets utilisés lors des tests nécessite un nouvel agrément.

II. — Un dispositif de neutralisation de billets intégré aux automates bancaires répond aux conditions suivantes :

1° Le dispositif est conçu pour rendre impropre à leur destination les billets de banque contenus dans un coffre d'automate bancaire en cas de tentative d'attaque ;

2° Le dispositif intègre ou non des capteurs permettant de détecter les modes d'attaque ;

3° Le dispositif est équipé d'un mécanisme qui se déclenche en cas de tentative d'effraction du corps du coffre ou de la porte, d'ouverture non autorisée de la porte, d'arrachement du coffre ou d'attaque à l'explosif solide, liquide ou gazeux de l'automate ;

4° Le déclenchement du mécanisme neutralise la totalité des billets de façon immédiate et définitive ;

5° La neutralisation affecte au moins 20 % de chaque face de chacun des billets de banque ; elle est irréversible et reconnaissable de façon évidente par les utilisateurs ;

6° Les substances ou éléments utilisés pour assurer la neutralisation des billets contiennent un ou plusieurs éléments traceurs permettant de caractériser de façon unique leur origine ainsi que l'automate bancaire concerné.

III. — Un arrêté du ministre de l'intérieur fixe :

1° Les caractéristiques techniques auxquelles satisfont les dispositifs de neutralisation de billets, notamment les informations qu'enregistre le système de programmation dont ils sont dotés, les caractéristiques des substances ou éléments utilisés pour assurer la neutralisation des billets et celles des éléments traceurs qu'ils contiennent ;

2° La nature des tests de résistance à la fraude et de neutralisation auxquels les dispositifs sont soumis ;

3° La composition du dossier de demande d'agrément.

IV. — Aux fins d'agrément des dispositifs de neutralisation importés des autres Etats membres de l'Union européenne ou parties à l'accord sur l'Espace économique européen, sont acceptés les rapports d'essais et les certificats établis par un organisme agréé ou accrédité dans ces Etats qui attestent la conformité de ces dispositifs à des conditions techniques et réglementaires assurant un niveau de protection équivalent à celui prévu par le présent décret et l'arrêté mentionné au III.

Article 9 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 12
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I. - La commission technique consultée sur les demandes d'agrément mentionnées aux articles 8-1 et 8-2 comprend :
1° Un représentant du ministère de l'intérieur, président, nommé par arrêté du ministre de l'intérieur ;
2° Le directeur général de la police nationale ou son représentant ;
3° Le directeur général de la gendarmerie nationale ou son représentant ;
4° Un membre désigné par le ministre chargé des transports ;
5° Un représentant de la Banque de France, désigné par le gouverneur ;
6° Une personne qualifiée en matière de sécurité des transports de fonds, désignée par le ministre de l'intérieur.
Les membres mentionnés aux 1°, 4°, 5° et 6° peuvent avoir un suppléant désigné dans les mêmes conditions.
Les membres de la commission exercent leurs fonctions à titre gratuit. Toutefois, leurs frais de déplacement et de séjour peuvent être remboursés dans les conditions prévues par la réglementation applicable aux personnels civils de l'Etat.
II. - Peuvent assister aux travaux de la commission, avec voix consultative :
1° Un représentant de la Fédération bancaire française ;
2° Un représentant de la Fédération des entreprises de la sécurité fiduciaire ;
3° Un représentant des laboratoires reconnus par l'Etat chargés des vérifications et des tests des dispositifs de neutralisation de valeurs, désigné par le ministre de l'intérieur sur proposition de ces laboratoires.

Article 9-1 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 13
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Le silence gardé pendant plus de quatre mois sur la demande d'agrément d'un dispositif mentionné à l'article 8-1 ou à l'article 8-2 vaut décision de rejet.

Article 10 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 14
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Lorsque le transport est effectué au moyen d'un véhicule blindé, chaque convoyeur doit être autorisé à porter l'une des armes définies au premier alinéa de l'article 3.
L'autorisation de port d'arme est délivrée pour une durée de cinq ans.
La demande d'autorisation de port d'arme est présentée par l'entreprise qui emploie le convoyeur.
L'autorisation de port d'arme est délivrée par le préfet du département où l'entreprise a son principal établissement ou, le cas échéant, son établissement secondaire, et dans le cas où cet établissement est situé à Paris, par le préfet de police.
Le dossier de demande comporte, outre la copie d'une pièce d'identité en cours de validité, le justificatif de l'aptitude professionnelle, le numéro de carte professionnelle attribuée par la commission régionale d'agrément et de contrôle, ainsi qu'un certificat médical datant de moins de quinze jours, placé sous pli fermé et attestant que l'état de santé physique et psychique du convoyeur n'est pas incompatible avec le port d'une arme.
L'autorisation de port d'arme devient caduque en cas de retrait de la carte professionnelle ou si son titulaire cesse d'être employé comme convoyeur par l'entreprise qui a présenté la demande d'autorisation, sauf en cas de reprise d'activités et de personnels de cette entreprise par une autre entreprise de transport de fonds. Le nouvel employeur informe immédiatement le préfet mentionné au troisième alinéa de cette nouvelle situation.

Article 11 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2013-723 du 12 août 2013 - art. 6
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Les autorisations de détention d'armes sont délivrées à l'entreprise par le préfet du département dans lequel se trouve son siège social.

En dehors de l'exécution des missions, les armes, éléments d'armes et munitions doivent être conservés dans les conditions prévues à l'article 114 du décret du 30 juillet 2013 susmentionné.

Article 12 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2012-1109 du 1er octobre 2012 - art. 15
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I.-Il est institué, dans le département, une commission départementale de la sécurité des transports de fonds.

La commission départementale est saisie pour avis, dans les cas et selon les modalités prévues par le décret pris en application de l'article L. 613-10 du code de la sécurité intérieure, de certains des aménagements et dispositifs envisagés par les entreprises de transport de fonds et par les personnes faisant appel, de façon habituelle, à de telles entreprises.
Le préfet peut consulter la commission sur toute question relative à la collecte des fonds ou au transport des fonds, bijoux et métaux précieux et sur toute question portant sur les locaux et automates bancaires desservis.
II.-La commission départementale de la sécurité des transports de fonds est présidée par le préfet et, à Paris, par le préfet de police. Elle comprend en outre :
1° Des représentants des services de l'Etat dans le département désignés par le préfet ;
2° Le directeur départemental de la Banque de France ;
3° Deux maires désignés par l'association départementale des maires ;
4° Deux représentants locaux des établissements de crédit, désignés par le préfet sur proposition de l'Association française des établissements de crédit et des entreprises d'investissement ;
5° Deux représentants des établissements commerciaux de grande surface, désignés par le préfet sur proposition des organisations professionnelles représentatives ;
6° Un représentant des professions de la bijouterie, désigné par le préfet sur proposition des organisations professionnelles représentatives ;
7° Deux représentants des entreprises de transport de fonds, désignés par le préfet sur proposition des organisations professionnelles représentatives ;
8° Deux convoyeurs de fonds, désignés par le préfet sur proposition des organisations syndicales représentatives des salariés sur le plan départemental.
La commission se réunit au moins une fois par an. Elle peut entendre toute personne dont l'audition lui paraît utile.
Les procureurs de la République près les tribunaux de grande instance ayant leur siège dans le département sont informés des réunions de la commission, ainsi que des avis émis par celle-ci. Ils participent, sur leur demande, à ses réunions.
NOTA :

Décret 2006-665 2006-06-07 art. 61 : Spécificité d'application.

Article 12-1 (abrogé au 1 décembre 2014)

- Créé par Décret n°2012-1109 du 1er octobre 2012 - art. 16
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16
- Il est créé, pour une durée de cinq ans, une Commission nationale consultative de la sécurité des transports de fonds, placée auprès du ministre de l'intérieur.

Article 12-2 (abrogé au 1 décembre 2014)

- Modifié par DÉCRET n°2014-901 du 18 août 2014 - art. 35
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

I. — La commission étudie les problèmes spécifiques que connaissent les professionnels du transport de fonds, bijoux et métaux précieux et fait des propositions en vue d'améliorer leur sécurité.
Elle fait notamment toute recommandation portant sur les modes de transport des fonds

d’une valeur inférieure à 30 000 euros, en tenant compte des attaques et agressions survenues et des tentatives constatées.
II. — Elle peut être saisie pour avis :
1° Par le ministre de l’intérieur sur tout projet de texte législatif ou réglementaire en matière de transport de fonds, bijoux et métaux précieux et sur toute question soulevée, notamment par une commission départementale de la sécurité des transports de fonds, dans ce domaine ;
2° Par un tiers de ses membres, sur toute question relevant de son champ de compétence.
III. — La commission est informée annuellement par le Conseil national des activités privées de sécurité des résultats des missions de contrôle des entreprises de transport de fonds.
IV. — Elle établit et transmet chaque année au ministre de l’intérieur un rapport :
1° Retraçant le bilan de ses travaux et propositions ;
2° Recensant les expériences innovantes contribuant à une meilleure sécurité des transports de fonds, bijoux et métaux précieux.

Article 12-3 (abrogé au 1 décembre 2014)

- Modifié par DÉCRET n°2014-901 du 18 août 2014 - art. 36
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

La Commission nationale consultative de la sécurité des transports de fonds est présidée par le délégué aux coopérations de sécurité au ministère de l’intérieur, par son représentant ou par un autre représentant du ministre de l’intérieur.
Elle comprend en outre des représentants de l’administration, dont le directeur général du Trésor ou son représentant et le directeur général des infrastructures des transports et de la mer ou son représentant, des représentants des communes désignés par l’Association des maires de France, des représentants de la Banque de France, des entreprises de transport de fonds, des entreprises prestataires de services pour automates bancaires, des salariés du transport de fonds, des établissements de crédit, des entreprises du secteur de l’assurance, des commerçants et des centres commerciaux, des professions de la bijouterie, de l’horlogerie, du travail et du négoce des métaux précieux et d’associations ou de groupements professionnels dont l’activité concourt au renforcement de la sécurité des transports de fonds.
La composition de la commission est précisée par arrêté du ministre de l’intérieur.

Article 12-4 (abrogé au 1 décembre 2014)

- Modifié par DÉCRET n°2014-901 du 18 août 2014 - art. 37
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

La commission se réunit au moins deux fois par an. Son secrétariat est assuré par les services du ministère de l’intérieur.

Article 12-5 (abrogé au 1 décembre 2014)

- Créé par Décret n°2012-1109 du 1er octobre 2012 - art. 16
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16
- Les membres de la commission exercent leurs fonctions à titre gratuit.

Article 13 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2004-295 du 29 mars 2004 - art. 6 JORF 30 mars 2004
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Le fait de contrevenir aux dispositions des articles 2 à 8-1 et 10 est puni de l'amende prévue pour les contraventions de la 5e classe.

Le fait de faciliter sciemment, par aide ou assistance, la préparation ou la commission des infractions prévues à l'alinéa précédent est puni de la même peine.

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues à l'article 121-2 du code pénal, des infractions définies au présent article. La peine encourue par les personnes morales est l'amende, suivant les modalités de l'article 131-41 du code pénal.

La récidive des infractions prévues au présent article est réprimée conformément aux articles 132-11 et 132-15 du code pénal.

Article 14 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2004-295 du 29 mars 2004 - art. 7 JORF 30 mars 2004
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Les dispositions relatives à l'équipage des véhicules banalisés mentionnés à l'article 2 dans sa rédaction issue du décret n° 2004-295 du 29 mars 2004 entrent en vigueur à l'expiration d'un délai de six mois à compter de la publication dudit décret au Journal officiel de la République française.

Article 15 (abrogé au 1 décembre 2014)

- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Les convoyeurs de fonds titulaires d'un agrément à la date de publication du présent décret conservent le bénéfice de cet agrément. Leur autorisation de port d'arme reste valable jusqu'à la date de son expiration.

Article 16 (abrogé au 1 décembre 2014)

- Modifié par Décret n°2011-338 du 29 mars 2011 - art. 17 (V)
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Le présent décret est applicable à Mayotte, sous réserve des adaptations suivantes :

1° (Alinéa abrogé).

2° Le premier alinéa de l’article 3 est remplacée par la phrase suivante :

Chacune des personnes mentionnées aux 1° et 2° du I de l’article 2 porte une arme dont la catégorie est définie par le préfet, ainsi que les munitions correspondantes.

Le second alinéa du même article est remplacé par un alinéa ainsi rédigé :

Tout véhicule blindé est en outre équipé d’une arme dont la catégorie est définie par le préfet, ainsi que des munitions correspondantes. ;

3° (Alinéa abrogé).

4° Le cinquième alinéa de l’article 10 est remplacé par un alinéa ainsi rédigé :

L’agrément et l’autorisation de port d’arme sont délivrés par le préfet ;

5° Le premier alinéa de l’article 11 est remplacé par un alinéa ainsi rédigé :

Les autorisations de port d’arme sont délivrées à l’entreprise par le préfet ;

6° L’article 12 est remplacé par les dispositions suivantes :

I.-Il est créé à Mayotte une commission de la sécurité des transports de fonds.

La commission peut être consultée sur toute question relative à la sécurité des collectes et transports de fonds à Mayotte, ainsi qu’à la sécurité du traitement des moyens de paiement par les entreprises.

II.-La commission de la sécurité des transports de fonds est présidée par le préfet. Elle comprend en outre :

1° Des représentants des services de l’Etat désignés par le préfet ;

2° Le directeur de l’agence de Mayotte de l’Institut d’émission des départements d’outre-mer ;

3° Deux maires désignés par l'Association des maires de Mayotte ;

4° Deux représentants locaux des établissements de crédit, désignés par le préfet ;

5° Deux représentants des établissements commerciaux de grande surface, désignés par le préfet ;

6° Deux représentants des entreprises de transport de fonds, désignés par le préfet ;

7° Deux convoyeurs de fonds, désignés par le préfet.

Le procureur de la République près le tribunal de grande instance est informé des réunions de la commission, ainsi que des avis émis par celle-ci. Il participe, sur sa demande, à ses réunions.

NOTA :

Décret 2006-665 2006-06-07 art. 61 : Spécificité d'application.

Article 16-1 (abrogé au 1 décembre 2014)

· Créé par Décret n°2009-650 du 9 juin 2009 - art. 6
· Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Pour l'application des dispositions du présent décret à Saint-Barthélemy et à Saint-Martin, l'article 12 est ainsi modifié :
1° Les mots : "commission départementale" sont remplacés par les mots : "commission territoriale" ;
2° Dans le I, les mots : ", dans le département, " sont remplacés par les mots : ", à Saint-Barthélemy et à Saint-Martin," ;
3° Le 2° du II est ainsi rédigé :
"2° Le directeur de l'agence de l'Institut d'émission des départements d'outre-mer" ;
4° Le 3° du II est ainsi rédigé :
"3° Le président du conseil territorial et un conseiller territorial désigné par le conseil territorial ; ".

Article 17

A modifié les dispositions suivantes :
· Modifie Décret n°86-1099 du 10 octobre 1986 - art. 7 (V)
· Modifie Décret n°95-589 du 6 mai 1995 - art. 26 (VT)

Article 17-1 (abrogé au 1 décembre 2014)

- Créé par Décret n°2011-1919 du 22 décembre 2011 - art. 56
- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16
- Le présent décret est applicable en Polynésie française sous réserve des adaptations suivantes :

1° A l'article 1er, les valeurs de 30 000 euros et de 100 000 euros sont remplacées respectivement par les valeurs de 3 579 900 francs Pacifique et de 11 933 000 francs Pacifique, et la référence aux articles du code des postes et télécommunications est remplacée par la référence aux dispositions applicables localement ;

2° Aux articles 3 et 11, la référence au décret du 6 mai 1995 est remplacée par la référence au décret n° 2009-450 du 21 avril 2009 ;

3° Aux articles 10 et 16, la référence à la commission régionale d'agrément et de contrôle instituée à l'article 33-5 de la loi du 12 juillet 1983 est remplacée par la référence à la commission locale d'agrément et de contrôle de Polynésie française mentionnée à l'article 36 du décret n° 2011-1919 du 22 décembre 2011 ;

4° L'article 12 est ainsi rédigé :

I. — Il est institué une commission de la sécurité des transports de fonds. La commission peut être consultée sur toute question relative à la sécurité des collectes et transports de fonds en Polynésie française, ainsi qu'à la sécurité du traitement des moyens de paiement par les entreprises.

II. — La commission de la sécurité des transports de fonds est présidée par le haut-commissaire de la République. Elle comprend en outre :

1° Des représentants des services de l'Etat désignés par le haut-commissaire ;

2° Le directeur de l'agence de Polynésie française de l'Institut d'émission des départements d'outre-mer ;

3° Deux représentants du syndicat pour la promotion des communes de Polynésie française ;

4° Deux représentants locaux de la fédération des banques, désignés par le haut-commissaire ;

5° Deux représentants des entreprises de transports de fonds, désignés par le haut-commissaire ;

6° Deux convoyeurs de fonds, désignés par le haut-commissaire.

Le procureur de la République près le tribunal de première instance est informé des réunions de la commission ainsi que des avis émis par celle-ci. Il participe, sur sa demande, à ces réunions.

Article 18 (abrogé au 1 décembre 2014)

- Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Le décret n° 79-618 du 13 juillet 1979 relatif à la protection des transports de fonds est abrogé.

Article 19 (abrogé au 1 décembre 2014)

· Abrogé par DÉCRET n°2014-1253 du 27 octobre 2014 - art. 16

Le ministre de l'économie, des finances et de l'industrie, le garde des sceaux, ministre de la justice, le ministre de l'intérieur, le ministre de la défense, le ministre de l'équipement, des transports et du logement et le secrétaire d'Etat à l'outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Lionel Jospin

Par le Premier ministre :

Le ministre de l'intérieur,

Jean-Pierre Chevènement

Le ministre de l'économie,

des finances et de l'industrie,

Laurent Fabius

Le garde des sceaux, ministre de la justice,

Élisabeth Guigou

Le ministre de la défense,

Alain Richard

Le ministre de l'équipement,

des transports et du logement,

Jean-Claude Gayssot

Le secrétaire d'Etat à l'outre-mer,

Jean-Jack Queyranne

NOTA :
Décret n° 2009-621 du 6 juin 2009 article 1 : Les dispositions réglementaires instituant les commissions administratives à caractère consultatif dont la liste est annexée au présent décret sont prorogées pour une durée de cinq ans (Commission technique consultative sur les demandes d'agrément des dispositifs de nouvelles technologies et de transports de fonds).
Conformément à l'article 1 du décret n° 2014-597 du 6 juin 2014, la Commission technique consultative sur les demandes d'agrément des dispositifs de nouvelles technologies et de transports de fonds est renouvelée jusqu'au 8 juin 2015.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Circulaire du 14 septembre 2011 relative au cadre juridique applicable à l'installation de caméras de vidéoprotection sur la voie publique et dans des lieux ou établissements ouverts au public, d'une part, et dans des lieux non ouverts au public, d'autre part

NOR : *PRMX1124533C*

Paris, le 14 septembre 2011

Le Premier ministre, à Monsieur le ministre d'Etat, Mesdames et Messieurs les ministres, Mesdames et Messieurs les secrétaires d'Etat, Mesdames et Messieurs les préfets de département, Mesdames et Messieurs les recteurs d'académie,

1. *Le visionnage de la voie publique ou de lieux et établissements ouverts au public par des caméras de vidéoprotection*

Les systèmes de vidéoprotection mis en œuvre sur la voie publique ou dans des lieux et établissements ouverts au public (1) relèvent du régime juridique fixé par les articles 10 et 10-1 de la loi nº 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. L'installation de tels systèmes de vidéoprotection est soumise à l'obtention d'une autorisation préfectorale prise après avis de la commission départementale de la vidéoprotection, présidée par un magistrat judiciaire.

Par exception, le I de l'article 10 susmentionné prévoit que les systèmes dont les images sont utilisées « dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques » sont soumis à la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Comme le précise le Conseil d'Etat dans un avis du 24 mai 2011, les dispositifs de vidéoprotection ne relèvent de cette exception et ne doivent donc être soumis à la Commission nationale de l'informatique et des libertés – CNIL –, préalablement à leur installation, que si les traitements automatisés ou les fichiers dans lesquels les images sont utilisées sont organisés de manière à permettre, par eux-mêmes, l'identification des personnes physiques, du fait des fonctionnalités qu'ils comportent (reconnaissance faciale notamment).

En revanche, le seul fait que les images issues de la vidéoprotection puissent être rapprochées, de manière non automatisée, des données à caractère personnel contenues dans un fichier ou dans un traitement automatisé tiers (par exemple, la comparaison d'images enregistrées et de la photographie d'une personne figurant dans un fichier nominatif tiers) ne justifie pas que la CNIL soit saisie préalablement à l'installation du dispositif de vidéoprotection lui-même.

2. *Le visionnage des lieux non ouverts au public par des caméras de vidéoprotection*

Les dispositions de la loi du 21 janvier 1995 ne s'appliquent pas aux systèmes de vidéoprotection installés dans des lieux non ouverts au public, comme les parties communes des immeubles d'habitation, les locaux professionnels et les établissements affectés à l'enseignement ou à la garde d'enfants.

Saisi pour avis du cadre juridique applicable aux systèmes de captation et d'enregistrement d'images recueillies pour assurer la sécurité des établissements pénitentiaires, le Conseil d'Etat a relevé, dans son avis du 24 mai 2011 déjà mentionné, qu'un dispositif de surveillance au moyen de caméras peut parfois constituer un traitement automatisé de données à caractère personnel soumis à la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. En effet, les dispositifs de vidéoprotection captent des images qui, si elles ne constituent pas par elles-mêmes des données à caractère personnel, livrent des informations sur les personnes qui y apparaissent, notamment leur présence en un endroit et à un moment déterminés. Lorsque ces personnes sont identifiables, les deux éléments constitutifs de la notion de « donnée à caractère personnel » sont réunis.

Aux termes de cet avis, un système de vidéoprotection utilisé dans des locaux non ouverts au public constitue ainsi un traitement automatisé de données à caractère personnel soumis aux dispositions de la loi du 6 janvier 1978, dès lors que deux conditions cumulatives sont remplies :

– d'une part, les images font l'objet d'un enregistrement et d'une conservation, et non d'un simple visionnage. Le seul fait de capter les images au moyen d'une caméra et de les visionner en temps réel sans procéder à un enregistrement (2) ne constitue pas un traitement et ne relève pas des dispositions de la loi « informatique et libertés » mais des seules règles relatives à la protection de la vie privée (articles 9 du code civil et 226-1 du code pénal) et, le cas échéant, des dispositions du code du travail si les caméras sont installées dans des locaux professionnels ;
– d'autre part, le responsable du traitement ou les agents ayant accès aux enregistrements ou ayant vocation à y accéder sont en mesure, par les moyens dont ils disposent normalement, d'identifier les personnes filmées. L'identification des personnes est considérée comme possible dès lors que le système est mis en œuvre dans des lieux habituellement fréquentés par des personnes dont une partie significative est connue du responsable du système de vidéoprotection ou des personnes ayant vocation à visionner les images enregistrées.

Sur ce dernier point, il y a lieu de considérer que les systèmes comportant des caméras d'enregistrement filmant des lieux non ouverts au public relèvent de la loi du 6 janvier 1978, et ainsi de la compétence de la Commission nationale de l'informatique et des libertés, lorsqu'un nombre significatif des personnes filmées sont connues de celles qui ont accès aux images. Tel sera le cas des systèmes de vidéoprotection installés dans des lieux pour lesquels le responsable du système dispose par ailleurs d'un moyen d'identification tel qu'un trombinoscope (locaux professionnels, établissements pénitentiaires...) ou dans des lieux où sont appelées à se trouver habituellement des personnes dont une partie significative est connue par les personnes ayant accès aux images (établissements scolaires, établissements hospitaliers...).

Dès lors que les deux conditions rappelées ci-dessus sont remplies, il y a lieu de procéder aux formalités préalables auprès de la CNIL.

*
* *

Vous vous assurerez de la déclaration ou de la demande d'autorisation à la Commission nationale de l'informatique et des libertés des systèmes de vidéoprotection installés dans des lieux non ouverts au publics et répondant aux conditions mentionnées au point 2. Je vous rappelle qu'en application des articles 22 à 27 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés la finalité poursuivie par le système de vidéoprotection constitue le critère déterminant les formalités préalables à la mise en œuvre du traitement.

Ainsi, l'acte réglementaire créant un système de vidéoprotection mis en œuvre par une autorité publique dans un lieu non ouvert au public sera soumis à la procédure d'autorisation prévue à l'article 26 de la loi du 6 janvier 1978 s'il participe à la protection de la sûreté de l'Etat, de la défense ou de la sécurité publique ou s'il vise la prévention ou la poursuite d'infractions pénales. En revanche, les systèmes usuels de vidéoprotection installés dans des locaux professionnels relèvent en général d'une simple déclaration auprès de la CNIL sur le fondement de l'article 23 de la loi « informatique et libertés ».

J'appelle enfin votre attention sur les systèmes de vidéoprotection pouvant être qualifiés de « mixtes » parce qu'ils traitent à la fois des images prises dans des lieux non accessibles au public et des images prises dans des lieux ouverts au public ou sur la voie publique. Dans ce cas, il y aura lieu de faire application à la fois de la loi du 21 janvier 1995 et de la loi du 6 janvier 1978. Vous veillerez donc à saisir le préfet territorialement compétent pour obtenir une autorisation préalable à l'installation d'un système et à procéder auprès de la Commission nationale de l'informatique et des libertés à la formalité préalable applicable.

Le dossier transmis au préfet sera composé conformément aux prescriptions de l'article 1er du décret n° 96-926 du 17 octobre 1996, pris pour l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995. La demande de saisine de la CNIL devra quant à elle comporter les indications prévues à l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le préfet et la CNIL examineront les demandes chacun pour ce qui le concerne et au regard des seules règles qu'il ou elle a compétence pour appliquer.

Je vous remercie d'assurer la plus large diffusion de la présente circulaire.

Pour le Premier ministre et par délégation :
Le secrétaire général du Gouvernement,
SERGE LASVIGNES

(1) Constituent des lieux ouverts au public les lieux dont l'accès est libre (plages, jardins publics, promenades publiques, commerces...) ainsi que les lieux dont l'accès est possible, même sous condition, dans la mesure où toute personne qui le souhaite peut remplir cette condition (paiement d'un droit d'entrée, par exemple au cinéma).

(2) L'enregistrement seul d'images, sans conservation, ne saurait justifier l'application des dispositions de la loi « informatique et libertés ». Les systèmes permettant un visionnage des images avec un différé de quelques minutes n'ont donc pas à être soumis pour avis ou pour autorisation à la CNIL.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

cerfa
N° 51336#02

NOTICE D'INFORMATION

relative au formulaire CERFA n° 13806*03 et 14095*02

Demande d'autorisation d'un système de vidéoprotection

A) Informations générales

A-1) L'encadrement juridique :

L'usage de la vidéoprotection est régi par **les articles L.223-1 à L.223-9, L.251-1 à L.255-1 et L.613-13 du code de la sécurité intérieure et par le décret d'application n°96-926 du 17 octobre 1996.** Les conditions d'application de ces textes sont explicitées par les circulaires : **INTD9600124C du 22 octobre 1996, INTD0600096C du 26 octobre 2006 et INTK0930018J du 2 février 2009.**

Dans les lieux privatifs ou les locaux à usage exclusivement professionnel qui n'accueillent pas de public au sens de la loi, la réglementation de la vidéoprotection mentionnée ci-dessus n'est pas applicable. La mise en place éventuelle de caméras doit cependant s'effectuer dans le respect de la vie privée et sans visionner la voie publique.

Les dispositions générales du code civil sur le droit à l'image (article 9) ou des réglementations particulières, telle que celle du code du travail **(3ème alinéa de l'article L. 2223-32 et articles L. 1222-4 et L.1221-9)** sont alors applicables.

L'article 226-1 du code pénal punit d'un an d'emprisonnement et de 45 000 € d'amende toute personne ayant volontairement porté atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant l'image d'une personne se trouvant dans un lieu privé, c'est-à-dire, selon la jurisprudence, un lieu qui n'est ouvert à personne sauf autorisation de celui qui l'occupe d'une manière permanente ou temporaire.

Dans les cas très rares où le système de vidéoprotection est relié à un traitement de données automatisées (fichier de données à caractère personnel), la loi « informatique et libertés » n°78-17 du 6 janvier 1978 est alors applicable. Dans ce cas précis, vous devez adresser une déclaration spécifique à la CNIL. (En cas de doute n'hésitez pas à poser votre question à l'adresse ci-après, une réponse vous sera adressée en retour dans les 10 jours : videoprotection@interieur.gouv.fr. Vous pouvez également prendre contact avec l'accueil de la préfecture qui instruira votre demande).

A-2) Dans quels cas devez vous déposer une demande d'autorisation ?

➢ *DANS LE CAS D'UN SYSTÈME VISÉ PAR LA LOI INSTALLÉ EN VOIE PUBLIQUE OU DANS UN LIEU OU UN ÉTABLISSEMENT OUVERT AU PUBLIC :*

1) Quel système est visé par la loi ?

Il y a vidéoprotection toutes les fois que sont mis en œuvre au moins une caméra et un moniteur, c'est-à-dire un écran permettant la visualisation des images, même s'ils ne sont pas situés dans le même local, et lorsque les caméras, fixes ou mobiles, fonctionnent de manière permanente ou non, prennent des images, éventuellement de manière séquentielle ou aléatoire, qui peuvent être visionnées, en temps réel ou en différé, sur place ou dans un lieu distant, sur un écran de type télévision ou sur un écran d'ordinateur.

Ainsi, la prise de photographies n'est pas un système de vidéoprotection et ce, quelque soit la technique utilisée (appareil numérique). Par contre, un dispositif dans lequel des images sont enregistrées à l'occasion d'une intrusion ayant déclenché le fonctionnement de caméras, dans un poste de contrôle éloigné, correspond bien à la définition de la vidéoprotection. Dans ce cas, le dispositif participe en outre des activités dites de télésurveillance régies par les dispositions du livre VI du CSI.

La loi ne se prononce pas sur la technologie utilisée. Elle définit seulement les principales modalités de fonctionnement des systèmes et fixe des normes techniques (par arrêté du 3 août 2007- annexes techniques publiées au JO du 25 août 2007). Cette absence de détermination précise des caractéristiques des dispositifs de vidéoprotection a permis d'accompagner le développement des nouvelles technologies et d'appliquer la réglementation à des cas auxquels le législateur ne pouvait penser en 1995 (ex : utilisation des webcam).

Ainsi, les systèmes de vidéoprotection numériques dont les images sont transmises par internet et consultées, à distance, par les personnes responsables du système entrent dans le champ des dispositions du CSI. Le procédé numérique doit permettre le respect des garanties imposées par la loi.

Par contre, la diffusion sur internet d'images issues de webcams ne constitue pas un dispositif de vidéoprotection dans la mesure où il n'y a pas «visionnage» des images sur un écran appartenant au propriétaire de la webcam mais transmission directe sur internet.

2) Les lieux visés par la Loi :

Les dispositions du CSI relatives à la vidéoprotection déterminent les lieux dans lesquels un dispositif de vidéoprotection peut être installé. Il s'agit de :

- l'intérieur des **lieux et établissements ouverts au public ;**
- la **voie publique** limitée géographiquement :
- aux abords des bâtiments et installations publics ;
- aux abords immédiats des bâtiments et installations appartenant à des personnes physiques ou morales de droit privé en cas de risque d'attentat terroriste ;
- aux voies de circulation.

Concernant la voie publique, la vidéoprotection peut être mise en œuvre :

- par une personne publique, pour assurer soit la protection des bâtiments et installations publics et de leurs abords ; soit la sauvegarde des installations utiles à la défense nationale ; soit la régulation des flux de transport ; soit la constatation des infractions aux règles de la circulation ; soit la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le second alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ; soit la prévention d'actes de terrorisme ; soit la prévention des risques naturels ou technologiques ; soit le secours aux personnes et la défense contre l'incendie ; soit la sécurité des installations accueillant du public dans les parcs d'attraction.

- par une personne physique ou morale de droit privé pour visionner les abords immédiats de ses bâtiments ou installations (article L 223-1 du CSI) au titre de la finalité de prévention d'actes de terrorisme ;

- dans certains lieux revêtant une dimension ou une complexité particulières, le préfet peut autoriser qu'un périmètre de voie publique ou compris dans un établissement ou un lieu ouvert au public puisse être vidéoprotégé, dans les limites et le cadre des finalités imposées par la loi. Cette notion répond à une nécessité opérationnelle d'adaptation de la vidéoprotection puisqu'elle recouvre l'espace susceptible d'être situé dans le champ d'une ou plusieurs caméras.

Sont visées par la notion d'ensemble immobilier ou foncier complexe les lieux ouverts au public dans des zones à forte concentration urbaine ou touristique ou dont la configuration géographique et architecturale rend difficile l'intervention des services de sécurité ou de secours mais également dans des zones utilisées dans le cadre de manifestations exceptionnelles. Pourraient entrer dans ce champ, à titre d'exemple : la place de la Concorde, une cité composée de plusieurs immeubles à usage d'habitation, une zone rurale utilisée dans le cadre d'une manifestation d'une ampleur exceptionnelle, comme une rave-party.

A-3) Quels documents devez-vous joindre à votre demande et dans quels cas ?

1) Les documents constitutifs d'une demande d'autorisation :

*L'ensemble des documents décrits ci-dessous ne sont pas exigibles dans tous les cas. Veuillez vous reporter au **2**) afin d'identifier précisément la nature de votre demande.*

- Le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires le CERFA n° 14095*02 ;

- Le rapport de présentation : il s'agit d'un rapport spécial expliquant les finalités du projet au regard des objectifs définis par la loi et les techniques mises en œuvre, eu égard à la nature de l'activité exercée, aux risques d'agression ou de vol présentés par le lieu ou l'établissement à protéger ;

- Le plan de masse : Il s'agit d'un plan des lieux montrant les bâtiments du demandeur et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et de leurs ouvertures ;

- Le plan de détail : Il s'agit d'un plan à une échelle suffisante montrant le nombre, le positionnement des caméras ainsi que les zones couvertes par celles-ci ;

- Un plan du périmètre : Il s'agit d'un document qui peut se substituer au plan de détails et au plan de masse, montrant l'espace susceptible d'être situé dans le champ de vision d'une ou plusieurs caméras dans le cas d'une demande portant sur un périmètre à vidéoprotéger ;

- La description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images : théoriquement ces informations sont indiquées dans les parties 5,7 et 8 du formulaire mais en cas de dispositif élaboré notamment en cas de traitement par une société extérieure, un document expliquant le fonctionnement du système peut-être demandé.

- La désignation des personnes susceptibles d'accéder aux images (rubrique 6 du formulaire): il s'agit de toute personne habilitée par le responsable à accéder aux images et donc susceptible de les visionner (il peut s'agir bien sûr du responsable lui-même mais aussi du technicien de maintenance par exemple). Ce n'est que dans l'hypothèse où plus de 4 personnes sont habilitées à accéder aux images qu'il convient de joindre une liste complémentaire au formulaire de demande.

Dans l'hypothèse où une des personnes habilitée à accéder aux images relève d'une société privée agissant par délégation, il convient de joindre l'agrément de ce prestataire

- Modèle de l'affiche ou du panonceau d'information du public : les panonceaux destinés à informer d'un système sur la voie publique doivent comporter un pictogramme (dessin) représentant une caméra. Si les affiches ou panonceaux sont placés dans les lieux et établissements ouverts au public, le nom ou la qualité, ainsi que le numéro de téléphone du responsable auprès duquel toute personne intéressée peut s'adresser pour exercer son droit d'accès doivent y figurer.

Attestation de la conformité du système aux normes techniques définies par l'arrêté du 3 août 2007 : deux cas de figure se présentent. En fonction de l'installateur auquel vous aurez recouru vous devrez produire un des documents prévus à cet effet :

1) Si vous avez fait appel à un installateur certifié : une attestation de conformité établie par ce dernier suffit.

2) Si votre installateur n'est pas certifié : il vous faut produire un questionnaire précisant les caractéristiques techniques du dispositif et sa conformité aux normes techniques (voir modèle joint en Annexe 1).

2) Les documents à fournir en fonction des différents cas suivants :

Vidéoprotection de la voie publique avec désignation du nombre de caméras : veuillez joindre à votre dossier tous les documents énumérés en **1**) (sauf le plan du périmètre qui ne concerne que les cas de vidéoprotection d'un périmètre).

Vidéoprotection d'un périmètre (en voie publique ou dans un lieu ouvert au public) : veuillez founir le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires, le CERFA n° 14095*02, le rapport de présentation, le modèle d'affiche et/ou de panonceau d'information du public, le plan du périmètre, le justificatif de la conformité aux normes techniques (attestation de conformité par un installateur certifié ou questionnaire dans l'autre cas), description du dispositif (dans ce cas de figure ce descriptif sera limité aux techniques employées et aux modes de visionnage et d'exploitation des images **le nombre de caméras et leur emplacement n'auront pas à être indiqués)**. Eventuellement la liste complémentaire des personnes habilitées à accéder aux images si la partie 6 du formulaire ne suffit pas.

Vidéoprotection dans un lieu ou un établissement ouvert au public et 7 caméras maximum : le dossier dans ce cas est très simplifié : veuillez fournir le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires, le CERFA n°14095*02, l'affiche d'information et le justificatif de conformité si l'installateur n'est pas certifié (si vous avez fait appel à un installateur certifié, vous devez pouvoir produire son attestation en cas de contrôle mais n'êtes pas obligé de la transmettre dans le cas où vous effectuez votre déclaration par téléprocédure), éventuellement liste complémentaire des personnes habilitées à accéder aux images si la partie 6 du formulaire ne suffit pas.

Vidéoprotection dans un lieu ou un établissement ouvert au public et 8 caméras minimum : veuillez fournir le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires, le CERFA n° 14095*02, le rapport de présentation, le plan de détail, l'affiche d'information du public et le justificatif de conformité, éventuellement la liste complémentaire des personnes habilitées à accéder aux images si la rubrique 6 du formulaire ne suffit pas.

A-4) A qui devez-vous adresser votre dossier ?

A la préfecture du département dans lequel vous souhaitez installer le dispositif (par exemple pour une société dont le déclarant est à Paris mais qui veut installer un dispositif dans une de ses succursales située en Gironde, il faut adresser votre déclaration à la préfecture de Bordeaux). Dans le cas d'un dispositif qui concernerait plusieurs départements (exemple : réseau autoroutier), le dossier doit être déposé à la préfecture du siège de l'établissement demandeur.

Ce dossier peut être transmis soit sous forme papier par voie postale ou déposé à l'accueil de la préfecture qui instruira votre demande, soit par téléprocédure disponible sur le site «videoprotection.interieur.gouv.fr» qui propose par ailleurs un ensemble d'informations ou d'actualités sur le sujet de la vidéo protection.

B) Comment remplir le formulaire de demande d'autorisation ?

Vous devez indiquer le numéro du département où se trouve la préfecture compétente en complétant par trois chiffres la case prévue à cet effet en haut du formulaire CERFA (par exemple pour PARIS renseigner 075, pour Marseille indiquer 013).

Rubrique 1 - Nature de la demande

Veuillez cocher obligatoirement une des trois cases proposées correspondant à la nature de votre demande (par exemple s'il s'agit d'une première demande vous cocherez «demande initiale»).

En cas de demande de modification d'un dispositif existant ou de demande de renouvellement, préciser le numéro de dossier sous lequel il a été enregistré dans la partie prévue à cet effet.

La modification peut concerner par exemple l'augmentation du nombre de caméras ou la localisation de celles-ci, sauf, si l'autorisation obtenue portait sur un périmètre vidéoprotégé. Dans ce dernier cas vous devez simplement déclarer au préfet compétent soit par courrier soit par téléprocédure (sur le site «vidéoprotection.interieur.gouv.fr» à la rubrique «TELE-VIDEOPROTECTION» dans le menu «déclaration de mise en service») le nouveau positionnement de vos caméras. Si vous souhaitez, en revanche, modifier la définition du périmètre (changement de l'environnement de celui-ci), vous devez adresser une demande de modification complétée des documents nécessaires.

Rubriques 2 et 10 - Identité et fonction du déclarant

L'autorisation de mise en œuvre d'un système de vidéoprotection est délivrée à la personne responsable du système, c'est-à-dire à celle qui, ayant la capacité juridique pour ce faire, estime nécessaire de recourir à la vidéoprotection. L'obligation de déclaration des systèmes entrant dans le champ d'application des dispositions du CSI incombe à l'exploitant des lieux où sont installées les caméras, qu'il soit ou non le propriétaire des lieux et même lorsque le système de vidéoprotection n'est installé que pour une durée limitée. Le responsable n'est donc pas l'installateur.

Vous devez par conséquent impérativement compléter les informations relatives au nom, prénom et fonction du déclarant (la fonction se trouve à la rubrique 10 en fin de formulaire) **(Si par la suite, le responsable du système change, par exemple suite à une mutation ou un départ à la retraite, il faudra en aviser la préfecture, dans certains cas ce changement peut nécessiter une nouvelle demande d'autorisation ; la préfecture vous le précisera).**

Veuillez ensuite renseigner la dénomination (il peut s'agir d'une collectivité exemple : commune de XXX, d'une entreprise exemple : – SARL XXX- , d'un établissement privé ou public exemple : bibliothèque municipale de XXX ; ou institut XXX)

S'il existe un nom usuel différent de ce que vous avez indiqué, il est recommandé de l'indiquer à la ligne suivante qui reste une information facultative.

Concernant l'activité, elle doit être impérativement renseignée si la demande concerne une entreprise ou un lieu ouvert au public (exemple : musée, commerce de vêtements…).

Vous complèterez ensuite l'adresse de la collectivité, de l'établissement ou de l'entreprise (veuillez renseigner le plus précisément possible cette adresse en complétant toutes les rubriques proposées).

L'adresse électronique reste facultative, il est conseillé toutefois de la mentionner afin de faciliter les échanges le cas échéant, entre l'administration et le demandeur.

Rubrique 3 - Informations générales et finalité(s) du système de vidéoprotection

a) les informations générales :

Dans cette rubrique, vous devez compléter la partie relative aux horaires d'ouverture **sauf en cas de vidéoprotection sur la voie publique** (par exemple si vous déposez un dossier pour un commerce, cette information peut vous être réclamée en complément si vous ne la renseignez pas dès le départ).

De même, vous êtes invité à signaler les éventuelles agressions déjà survenues sur le lieu que vous souhaitez protéger ou les risques particuliers auxquels vous l'estimez exposé (délinquance de proximité, commerce recevant beaucoup de liquidités).

b) la ou les finalité(s) du système :

Veuillez cocher obligatoirement au moins l'une des cases proposées. Vous pouvez en cocher plusieurs, la finalité du système n'étant pas nécessairement unique. Si vous cochez la case «autre», vous devez préciser sur la ligne suivante le but que vous recherchez en installant un système de vidéoprotection.

Rubrique 4 - Localisation du système de vidéoprotection

Veuillez compléter soit la rubrique 4-1, soit la rubrique 4-2. En aucun cas vous ne pouvez compléter les deux rubriques en même temps (la rubrique 4-2 concerne uniquement les ensembles immobiliers ou fonciers de dimension importante ou complexes).

4-1 Lieu d'installation et nombre de caméras

Veuillez compléter le plus précisément possible l'adresse du lieu d'installation du dispositif (en cas d'installation sur la voie publique de plusieurs caméras réparties sur une certaine distance, veuillez indiquer au moins le nom de la voie).

Pour les dispositifs de 7 caméras maximum installées à l'intérieur d'un établissement, vous préciserez impérativement la superficie de cet espace intérieur.

4-2 Demande portant sur un périmètre

Il est possible, lorsque l'installation de vidéoprotection est prévue sur un ensemble foncier ou immobilier de dimension importante ou complexe, de recourir à la notion de périmètre vidéo protégé.

Cette formule présente l'avantage de vous dispenser du dépôt de demande de modification pour déplacer les caméras ou en augmenter le nombre à l'intérieur du périmètre.

Si vous souhaitez obtenir une autorisation au titre d'un périmètre vidéo protégé, veuillez préciser les différentes adresses (8 au maximum) qui constituent l'environnement de ce périmètre (par exemple si vous souhaitez une autorisation pour protéger une gare, vous préciserez à la rubrique 2 l'activité « gare » et indiquerez toutes les adresses permettant de délimiter le périmètre géographique dans lequel se trouve située cette gare).

Dans cette hypothèse c'est au moment où vous informerez le préfet de la mise en service des caméras que vous lui en préciserez la localisation.

Rubrique 5 - Caractéristiques du système

Vous devez préciser impérativement le nombre de jours pendant lesquels seront conservées les images. Ce chiffre (de 00 à 30 jours, délai de conservation maximum autorisé par la loi) sera reporté dans la case correspondante.

Vous répondrez ensuite à la question «existence d'un système de retransmission». Si vous cochez non, vous pouvez passer à la question relative à l'installateur. Si vous répondez oui, vous devrez cocher obligatoirement une des deux cases suivantes : retransmission en temps réel ou retransmission en temps différé.

Veuillez ensuite préciser, en cochant la case correspondante, si l'installateur auquel vous avez fait appel est certifié.

Si vous avez coché la case «oui» et que cet installateur est certifié par l'AFNOR-CNPP ou par un mécanisme de certification équivalent, Il faut mentionner le nom de cet installateur (ou de cette société d'installation) et son numéro de certification. Vous répondrez également à la question suivante en cochant «oui» ou «non». Si l'installateur vous a remis une attestation, vous n'êtes pas obligé de la joindre à votre dossier (pour les dispositifs importants de plus de 7 caméras ou en voie publique, il est toutefois conseillé de la joindre ; pour les petits dispositifs hors voie publique de 7 caméras maximum, vous n'êtes pas obligé de joindre au dossier cette attestation mais elle peut vous être réclamée en cas de contrôle a posteriori).

Si l'installateur n'est pas certifié, vous joindrez au dossier le questionnaire (dont le modèle figure, en annexe 1) précisant les caractéristiques du système.

Rubrique 6 - Personnes habilitées à accéder aux images

Il s'agit de mentionner le nom et prénoms des personnes qui seront en charge de visionner les images ou qui peuvent y accéder (s'il s'agit du responsable-déclarant de la demande d'autorisation lui-même, il convient de le préciser en réécrivant ses nom, prénoms et fonction qui devront dans ce cas correspondre aux informations contenues à la rubrique 2 et 10. De même, le ou les techniciens susceptibles d'intervenir sur le système au titre de la maintenance doivent être mentionnés dans cette liste. S'il y a plus de quatre personnes, il convient de joindre une liste complémentaire).

Si la ou les personnes habilitées à accéder aux images relèvent d'une société privée agissant par délégation, vous devez impérativement cocher la case « oui » prévue à cet effet.

En cas de modification de la liste des personnes habilitées, le signataire informera l'autorité préfectorale (soit par courrier, soit par « téléprocédure »).

Rubrique 7 - Traitement des images

Cette rubrique doit être renseignée dans le cas où les images font l'objet d'un traitement dans un lieu différent de celui de l'implantation des caméras et/ou par une personne autre que les responsables du système. Si ce n'est pas le cas, vous devez passer à la rubrique 8.

Rubrique 8 - Sécurité et confidentialité

La première ligne de cette rubrique doit impérativement être renseignée, il s'agit de décrire les mesures prises pour contrôler l'accès au poste central (code d'accès, porte blindée, badge d'accès, accès contrôlé).

Si vous avez coché la réponse «oui» à la question «existence d'un système d'enregistrement» en rubrique 5, veuillez répondre aux deux questions suivantes en décrivant 1) les mesures pour la sauvegarde et la protection des enregistrements (par exemple : armoire blindée) et 2) les modalités de destruction de ces enregistrements (par exemple : écrasement).

Rubrique 9 - Modalités d'information du public

Les textes en vigueur prévoyant l'obligation d'informer le public susceptible d'être filmé, vous préciserez les mesures prévues à cet effet.

Vous devez par conséquent compléter les deux lignes prévues dans cette rubrique.

Par ailleurs l'information sur l'existence d'un système de vidéoprotection devant être apportée au moyen de panonceaux comportant un pictogramme représentant une caméra (dans les cas de vidéoprotection sur la voie publique) et au moyen d'affiches ou de panonceaux (au choix en cas de vidéoprotection dans un lieu ou établissement recevant du public), n'oubliez pas de joindre à votre dossier le modèle d'affiche ou de panonceau.

Rubrique 10 - Service (ou personne) auprès duquel s'exerce le droit d'accès

L'article L.253-5 du code de la sécurité intérieure énonce :

« Toute personne intéressée peut s'adresser au responsable d'un système de vidéoprotection afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans le délai prévu. Cet accès est de droit. Un refus d'accès peut toutefois être opposé pour un motif tenant à la sûreté de l'Etat, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou au droit des tiers. »

Il s'agit de préciser auprès de quelle personne ou de quel service doit s'adresser une personne ayant été filmée par le dispositif que vous souhaitez installer pour vérifier les images.

Il vous appartient par conséquent de renseigner cette rubrique en indiquant soit le nom, prénom et fonction de la personne auprès de laquelle s'exerce ce droit d'accès aux images, soit le nom du service.

Vous pouvez compléter éventuellement ces quatre informations (nom, prénom, fonction, service auquel appartient cette personne).

Vous indiquerez ensuite l'adresse de cette personne et/ou de ce service (cela peut être la même personne que le déclarant-responsable du système).

La signature du formulaire

Veuillez, une fois les rubriques complétées, indiquer la fonction du signataire-déclarant (rubrique 2 du formulaire, page 4 de la présente notice), dater votre document et le signer en apposant, le cas échéant le cachet de la collectivité, de l'établissement ou de l'entreprise.

Si vous effectuez votre déclaration par téléprocédure, vous compléterez simplement la mention relative à la fonction du déclarant.

Annexe 1

cerfa
N° 51336#02

Questionnaire de conformité d'un système de vidéoprotection à l'arrêté du 3 aout 2007 portant définition des normes techniques des systèmes de vidéoprotection.

Je soussigné(e).....,
certifie par la présente que le système de vidéoprotection pour lequel j'ai sollicité une autorisation en date du....., installé par (nom et adresse de l'installateur)....
est conforme aux dispositions de l'arrêté du 3 août 2007.

Fait à …….....……., le …….....……

Caractéristiques du système (veuillez cocher les cases appropriées) :

1

Caractéristiques générales :

a. Nombre de caméras :

☐ moins de 8 caméras ☐ 8 caméras ou plus

b. Mode de fonctionnement du système :

☐ Le système comporte des caméras à plan large (destinées à une compréhension des situations) et des caméras à plan étroit (susceptibles de permettre une reconnaissance des individus)
☐ Le système ne comporte que des caméras à plan large
☐ Le système ne comporte que des caméras à plan étroit

2

Mode d'enregistrement des images :

a. Le stockage des images est-il ?

Analogique ☐ Numérique ☐

b. Possibilité de déterminer la caméra ayant filmé une scène :

Possible sur les enregistrements eux mêmes ☐
Possible grâce à un journal ☐
Non prévu ☐

c. Existe-t-il un journal gardant la trace des opérations effectuées sur les flux vidéo (export, modification, suppression)

Oui, journal manuel ☐
Oui, journal généré automatiquement sous forme électronique ☐
Non ☐

3

Questions relatives à la qualité des images :

a. La résolution des images en plan étroit (à l'exclusion de celles de régulation du trafic routier) est-elle toujours supérieure ou égale à 4 CIF (704 x 576 pixels) et le nombre d'images supérieur ou égal à 12 images/s

☐ Oui ☐ Non

b. La résolution des autres images est-elle toujours supérieure ou égale à 1CIF (352 x 288 pixels) et le nombre d'images supérieur ou égal à 6 images/s ?

☐ Oui ☐ Non

4

Transmission des images aux forces de police :

a. Les images peuvent-elles êtres exportées sans dégradation de leur qualité ?

Oui ☐ Non ☐

b. Dans le cas de systèmes numériques, si le format de codage des images n'est pas standard et libre de droits, le titulaire a-t-il prévu de fournir gratuitement à l'administration en cas de réquisition judiciaire, un système de lecture (ou une licence si le produit peut être installé » sur un PC standard) permettant de lire les enregistrements et d'effectuer les principales opérations de visualisation

Oui ☐ Non ☐

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Le Ministre

Paris, le 26 MAR 2015

Le ministre de l'intérieur

à

Monsieur le préfet de police
Mesdames et Messieurs les préfets de département
Monsieur le préfet de police des Bouches-du-Rhône

Copie pour information à
Monsieur le directeur général de la police nationale
Monsieur le directeur général de la gendarmerie nationale

CIRCULAIRE NOR : INTD1502555C

OBJET : Procédure de la levée de doute des télésurveilleurs

REF : Article L.613-6 du code de la sécurité intérieure

Résumé : Cette circulaire a pour objet de clarifier la procédure de la levée de doute imposée par la loi aux entreprises de télésurveillance afin de limiter, d'une part, les interventions injustifiées des forces de police ou de gendarmerie et, d'autre part, les risques de sanctions pécuniaires auxquels s'exposent les entreprises concernées. Vous pouvez utilement présenter cette méthodologie aux forces de police et de gendarmerie placées sous votre autorité.

L'article L.613-6 du code de la sécurité intérieure dispose que :

« *Est injustifié tout appel des services de la police nationale ou de la gendarmerie nationale par les personnes physiques ou morales exerçant des activités de surveillance à distance des biens meubles ou immeubles qui entraîne l'intervention indue de ces services, faute d'avoir été précédé d'une levée de doute consistant en un ensemble de vérifications, par ces personnes physiques ou morales, de la matérialité et de la concordance des indices laissant présumer la commission d'un crime ou délit flagrant concernant les biens meubles ou immeubles. L'autorité administrative peut prononcer à l'encontre des personnes physiques ou morales mentionnées à l'alinéa précédent qui appellent sans justification les services de la police nationale ou de la gendarmerie nationale une sanction pécuniaire d'un montant qui ne peut excéder 450 euros par appel injustifié.*

L'autorité administrative peut prononcer à l'encontre des personnes physiques ou morales mentionnées à l'alinéa précédent qui appellent sans justification les services de la police nationale ou de la gendarmerie nationale une sanction pécuniaire d'un montant qui ne peut excéder 450 euros par appel injustifié.

La personne physique ou morale à l'encontre de laquelle est envisagée la sanction pécuniaire prévue au précédent alinéa est mise en mesure de présenter ses observations avant le prononcé de la sanction et d'établir la réalité des vérifications qu'elle a effectuées, mentionnées au premier alinéa.

Cette sanction pécuniaire est recouvrée comme les créances de l'Etat étrangères à l'impôt et au domaine. Elle est susceptible d'un recours de pleine juridiction. »

La définition de la levée de doute consiste ainsi en un ensemble de vérifications, par les personnes physiques ou morales, de la matérialité et de la concordance des indices laissant présumer la commission d'un crime ou délit flagrant concernant les biens meubles ou immeubles.

Cette définition indique bien que la levée de doute est obligatoire dans le cadre de la commission d'un crime ou délit flagrant concernant les biens meubles et immeubles. Ainsi, dans le cas d'un crime ou d'un délit flagrant d'atteinte aux personnes, le texte ne prévoit pas une levée de doute effectuée par les télésurveilleurs.

Le fondement juridique de l'intervention des services de police et de gendarmerie est la procédure de flagrant délit puisque leur action se situe dans l'hypothèse d'un « crime ou d'un délit qui se commet actuellement ou qui vient de se commettre » prévue aux articles 53 et suivants du code de procédure pénale. Cette intervention correspond à une opération de police judiciaire.

Il est donc nécessaire que des indices apparents d'un comportement délictueux révélant une infraction répondant à la définition des crimes et délits flagrants existent préalablement à l'entrée des officiers et agents de police judiciaire dans les lieux surveillés à distance.

En raison de l'extrême sensibilité des détecteurs utilisés pour les systèmes d'alarmes « passifs » (détecteurs volumétriques, thermiques, capteurs de pression) engendrant de nombreux déclenchements intempestifs, la levée de doute pourrait répondre à la procédure suivante :

- en présence d'images non équivoques, confortées par l'existence d'éléments permettant de confirmer leur caractère inhabituel (liste des horaires de présence du personnel habilité, zones de passage autorisé, etc.) la réalité de l'atteinte aux personnes ou aux biens et immeubles est avérée et la levée de doute est réputée effectuée (CAA Versailles, 2014, n°13VE02603).

- en l'absence d'images non équivoques, une prise de contact avec le client est indispensable. Si le client est une entreprise, deux appels successifs peuvent être effectués auprès du ou des responsables déclarés afin de vérifier la situation. S'il s'agit d'un particulier, deux appels peuvent être réalisés dans les mêmes conditions auprès des personnes désignées par le contrat de prestation. Au terme de ces deux appels :

    - si la prise de contact avec le client a lieu, et se révèle fructueuse, la levée de doute est effectuée.

- si les tentatives de prise de contact avec le client se soldent par un échec, ou si un doute subsiste sur la commission d'un crime ou d'un délit flagrant concernant les biens meubles ou immeubles, il appartient à l'entreprise de télésurveillance de réaliser une vérification effective des causes du déclenchement des détecteurs par au moins deux éléments parmi les suivants : images vidéo, écoute des sons pouvant être émis dans le lieu surveillé, interaction phonique, concordance entre différentes alarmes, **ou,** en l'absence d'éléments concordants apparaissant à l'usage de ces procédés, par l'envoi d'un agent sur place. La levée de doute est alors réputée effectuée.

A votre initiative, pour répondre aux exigences des politiques de sécurité publique et raccourcir les délais d'intervention des forces de police et de gendarmerie, la procédure de levée de doute à mettre en œuvre peut être définie, localement, d'un commun accord entre les forces de l'ordre et les entreprises de télésurveillance pour des périodes et des lieux précis.

Par exemple, dans une zone délimitée, dans le cadre de la lutte contre les vols avec effraction, sur une période critique à préciser, il peut être convenu que les forces de sécurité intérieure seront sollicitées dès le déclenchement de l'alarme sur un site défini comme sensible (bijouterie, banque, entreprise de stockage de métaux, grande surface, etc.).

Enfin, dans la mesure où le délai de conservation des données images par les opérateurs de télésurveillance a été fixé à un mois maximum par l'article L.252-5 du code de la sécurité intérieure, il est recommandé aux services de la police et de la gendarmerie nationales de solliciter la transmission des données qui leur seraient nécessaires dans ce délai.

Vous veillerez à la diffusion de cette pratique, qui permettra de faciliter et de mieux définir les échanges entre les forces de sécurité intérieure et les entreprises chargées de la surveillance par des dispositifs électroniques.

Vous me rendrez compte, sous le timbre de la direction des libertés publiques et des affaires juridiques et de la délégation aux coopérations de sécurité, de toute difficulté rencontrée dans la mise en œuvre de cette circulaire.

Bernard CAZENEUVE

ANNEXE 2

PROTOCOLE D'ACCORD ENTRE

LE MINISTERE DE L'INTERIEUR

ET

LA FEDERATION FRANÇAISE DU BATIMENT

VISANT A LUTTER CONTRE LES VOLS ET AUTRES ACTES DELICTUEUX SUR CHANTIERS

Le Ministre de l'Intérieur,
Manuel VALLS

et

La Fédération Française du Bâtiment,
représentée par son président Didier RIDORET

Les vols sur les chantiers de bâtiment, dus notamment à l'envolée du coût des matières premières, constituent une préoccupation forte des professionnels et des pouvoirs publics ;

Ce phénomène, en dépit des actions déjà menées tant au sein de la profession que par les forces de sécurité intérieure, constitue un obstacle à l'effort de construction indispensable aux besoins de logements de nos concitoyens ;

La démarche de coopération entre les services de l'Etat, les maîtres d'ouvrage et les entreprises, mise en œuvre dans de nombreux départements en application d'un premier protocole conclu le 14 avril 2008, mérite d'être généralisée et accentuée afin de mieux combattre cette délinquance ;

Il est décidé par la présente convention de renouveler le cadre général de cette action concertée.

Définition de l'objectif

Article 1

Les professionnels du bâtiment et les pouvoirs publics se fixent pour objectif commun de conjuguer leurs efforts pour lutter plus efficacement contre les vols et atteintes volontaires visant les entreprises du bâtiment.

Une attention particulière est portée aux secteurs géographiques sensibles faisant l'objet d'une politique accrue de construction de logements sociaux afin d'offrir aux entreprises des conditions de travail satisfaisantes.

Mise en place d'un partenariat renforcé

Article 2

Le référent sûreté de la direction départementale de sécurité publique et du groupement de gendarmerie départementale, est l'interlocuteur privilégié des fédérations départementales du bâtiment.

Ces référents peuvent conseiller, participer à des actions de formation ou de sensibilisation collective, informer les entreprises et les maîtres d'ouvrage professionnels sur les caractéristiques du secteur d'implantation de leurs chantiers et solliciter des services territorialement compétents qu'ils organisent, de façon ponctuelle, des visites-conseils sur site.

Chaque département dispose de référents sûreté, policiers ou gendarmes, dont la liste actualisée des référents sûreté sera communiquée aux fédérations départementales.

Article 3

Les fédérations départementales du bâtiment informent les référents sûreté départementaux de l'ouverture de chantiers qu'elles considèrent comme sensible du point de vue de leur sécurité.

Le correspondant sûreté de chaque fédération départementale transmet au référent sûreté les coordonnées des entreprises retenues. Celles-ci recherchent avec le référent sûreté les modalités du dispositif le mieux adapté à mettre en œuvre pour prévenir les vols.

A cet effet, les entreprises renseignent une fiche navette, dont le modèle est annexé au présent protocole, transmise par le correspondant sûreté de la fédération départementale au référent sûreté concerné. Cette fiche, outre les informations générales concernant le chantier, doit contenir la liste des mesures de prévention envisagées sur le chantier objet du signalement.

Sur la base de cette fiche, le référent sûreté fait l'inventaire des menaces auxquelles ce chantier pourrait être confronté et évalue les mesures de prévention et de protection envisagées. Ces observations sont consignées dans la fiche navette retournée à l'entreprise.

Article 4

Les fédérations départementales, avec le soutien des référents sûreté, sensibilisent les entreprises à la sécurisation des chantiers : former des personnels aux enjeux de la sécurité, désigner un responsable sécurité, recourir aux dispositifs de prévention comme le gardiennage ou la vidéoprotection, élaborer des plans de limitation des risques pendant et hors les heures d'activité.

Conformément à la loi, il n'est pas utile de faire une démarche d'autorisation en préfecture lorsque les équipements de vidéoprotection sont installés dans l'enceinte du chantier sans visionner la voie publique. La mise en place des caméras doit cependant s'effectuer dans le respect de la vie privée.

Le ministère de l'intérieur sensibilisera tout particulièrement aux exigences de sûreté les entreprises adjudicatrices avec lesquelles il agit en qualité de maître de l'ouvrage ; les autres maîtres d'ouvrage publics ainsi que les maîtres d'ouvrage professionnels privés seront également sensibilisés à ces questions.

Lorsque le chantier est réputé sensible, le référent sûreté, policier ou gendarme, ou le correspondant sûreté de la FFB invitera les maîtres d'ouvrage concernés à renseigner la fiche "d'évaluation des menaces associées à une opération" afin de compléter l'analyse des risques et d'ajuster les mesures de prévention prévues dans la fiche navette.

Article 5

Le Ministère de l'Intérieur apporte son concours à la Fédération Française du Bâtiment pour la réalisation de supports matériels de communication, ou la diffusion de conseils dans ses publications professionnelles.

Prévention technique et opérationnelle

Article 6

Afin de lutter contre le vol de matériels particulièrement onéreux, la Fédération Française du Bâtiment, en liaison avec les sociétés d'assurances et les entreprises, incite au marquage d'identification ainsi qu'à tout moyen électronique de détection d'intrusion et à l'implantation de systèmes de géolocalisation sur les engins de chantier.

En liaison avec les exploitants des systèmes de géolocalisation, les forces de sécurité intérieure effectuent toutes les recherches appropriées pour retrouver les matériels dotés de dispositifs techniques préalablement installés.

Article 7

Les forces de sécurité intérieure prennent en compte, si nécessaire, dans leur maillage territorial de patrouilles, les chantiers réputés sensibles portés à leur connaissance. Elles conviennent le cas échéant de règles de signalement avec les personnels privés de gardiennage présents sur les sites.

Plaintes et investigations

Article 8

Afin de faciliter leurs démarches, les professionnels du bâtiment victimes de faits visés par la présente convention peuvent solliciter un référent sûreté départemental, ou l'interlocuteur local désigné, pour organiser un rendez-vous personnalisé avec l'interlocuteur de police ou de gendarmerie le plus adapté.

Article 9

Les services de police ou de gendarmerie intervenant pour des vols commis sur des chantiers procèdent, dans les 24 heures qui suivent le signalement, aux investigations de police technique et scientifique dès lors que des traces sont susceptibles d'être relevées.

Pour optimiser cette démarche, la Fédération Française du Bâtiment informe ses adhérents de la nécessité de conserver les lieux de vols et autres actes délictueux en état jusqu'au passage des personnels chargés des recherches de police technique et scientifique.

Déclinaison locale

Article 10

La présente convention peut être déclinée à l'échelle du département dans le cadre de conventions signées par les préfets, les responsables départementaux de la Fédération Française du Bâtiment et tout acteur de la chaîne de sécurité souhaitant s'y associer.

La lutte contre le vol sur les chantiers fait spécifiquement l'objet d'un volet dans les plans départementaux de sécurité, et d'une concertation dans le cadre des Conseils Locaux de Sécurité et de Prévention de la Délinquance.

La Fédération Française du bâtiment mobilise ses 57 000 entreprises adhérentes autour des engagements de la présente convention et ses déclinaisons locales.

A Paris, le 18 JAN. 2013

Le Ministre de l'Intérieur

Manuel VALLS

Le Président de la Fédération Française du Bâtiment

Didier RIDORET

Vols sur chantiers
Fiche navette
entreprise / correspondant sûreté / référent sûreté / entreprise

A transmettre au correspondant sûreté de la Fédération départementale
par fax au : .....
ou par mail à : .....

Partie 1. SIGNALEMENT D'UN CHANTIER « SENSIBLE » réservée à l'entreprise

1 - DECLARATION INITIALE (à remplir par l'entreprise et à transmettre correspondant sûreté de la FFB départementale)			Date :
PRESENTATION GENERALE DU CHANTIER :			
Adresse du chantier :		*Société, nom et téléphone du demandeur :* *(une seule entreprise doit être la porte parole des autres pour le chantier donné)* *(si nécessaire fournir un document à part)*	....
Nature de l'opération :	❑ Construction neuve ❑ Rénovation / Réhabilitation ❑ Réhabilitation locaux occupés ❑ Autre :	*Nom du Maître d'ouvrage et type d'activité de ce dernier :* *(si nécessaire fournir un document à part)*	....
Destination des locaux :	❑ Habitation ❑ Locaux bureaux ❑ Locaux commerces ❑ Locaux industriels ❑ Locaux mixtes ❑ Autre :	*Nom et téléphone du (des) contact(s) sur le site du chantier :* *(si nécessaire fournir un document à part)*	....
Superficie de l'emprise du chantier :	.....	*Heures normales de fonctionnement du chantier :*	.....
Date de début du chantier : *Durée prévisionnelle :*	....	*Nombre d'ouvriers maxi probable simultanément présents sur le chantier :*	.....

LE TRAITEMENT DU COURRIER ET DES LIVRAISONS SUSPECTS

Il s'agit de l'hypothèse de la réception de lettres ou de colis suspects éventuellement piégés (explosifs ou incendiaires, bactériologiques ou chimiques)

GÉNÉRALITÉS

Les lettres, paquets et colis peuvent être utilisés pour l'introduction de pièges ou de charges explosives, de substances chimiques ou bactériologiques.

En utilisant quelques procédures simples, il est aisé de réduire considérablement les risques dont celui de la non-détection d'un de ces envois.

LES LETTRES OU COLIS SUSPECTS EXPLOSIFS OU INCENDIAIRES

Ceux-ci peuvent être classés en deux catégories :

⇨ *envois reçus par l'intermédiaire de La Poste :*

- ils ne sont normalement pas équipés de systèmes de déclenchement (mise de feu ou piège) à retard, compte tenu en particulier de l'incertitude sur les délais d'acheminement, le fonctionnement du système s'effectue à partir de l'ouverture de la lettre ou du paquet et peut avoir un retard activé à cette occasion[1],

⇨ *envois reçus par porteur, coursier :*

- ils peuvent être équipés de système à retard.

A. Le courrier postal :

Il peut être contrôlé à partir de règles simples :

Les lettres et plis de faible épaisseur

a) l'origine et le destinataire sont mentionnés en toutes lettres. L'écriture est manuscrite, l'envoi est clos et l'enveloppe n'est pas du type à multi-ouvertures et fermetures possibles,

Aucune précaution à priori

[1] - Par exemple, par relâchement de la pression due au conditionnement de l'objet.

b) dans d'autres cas, l'ouverture est effectuée en tenant le contenu par les bords ; un contrôle visuel (éventuellement de l'odeur) précède le traitement normal du courrier afin de vérifier les anomalies (aspérités par exemple) éventuelles.

En cas de doute le traiter comme du courrier suspect (voir ci-après)

2 - Les lettres et plis épais :

- *s'ils sont souples et qu'aucune aspérité ou "bosse" n'est visible ou perceptible ou toucher, le traitement est le même que ci-dessus (1-a),*
- *s'ils sont rigides :*

⇨ du type décrit en 1-a aucune précaution a priori.

⇨ dans les autres cas, la possibilité d'un piégeage n'est pas à écarter.

L'ouverture doit être effectuée de telle sorte que la présence d'un système de déclenchement du piège soit détectée avant son fonctionnement

3 - Colis et paquets

Ils sont normalement rigides. Et si l'origine et le destinataire, voire la nature du contenu, ne sont pas mentionnés avec précision, des précautions sont à prendre à l'ouverture pour déceler la présence éventuelle d'un piège avant qu'il ne soit activé.

B. Courrier et paquets remis par porteur :

1 - Coursiers professionnels

On doit toujours pouvoir connaître l'expéditeur, puisqu'il a payé l'envoi, si cette indication n'est pas mentionnée sur le courrier, faire téléphoner par le coursier à son siège pour obtenir l'information.

Il faut refuser systématiquement le courrier dont l'origine n'est pas identifiée ou identifiable

2 - Porteurs occasionnels

Il s'agit souvent de personnels appartenant à l'administration ou à l'entreprise d'où vient le courrier.

Dans tous les cas, le courrier doit être identifié : origine reconnue, nom du destinataire, vérification auprès de celui qui attend du courrier ; s'il est absent et qu'il n'a pas laissé d'information à son entourage, prendre contact avec l'expéditeur.

Le courrier reçu par porteur ne doit pas être accepté s'il n'est pas parfaitement identifié

Il est en effet facile de piéger un paquet dont on connaît l'heure de livraison. Il peut être ainsi programmé pour que l'explosion de l'engin qu'il renferme (par exemple) ait lieu à un moment choisi, selon le but recherché.

Dans cette optique il n'est pas inutile de procéder au rappel de quelques notions élémentaires permettant de considérer qu'une lettre ou un colis sont des objets suspects.

Ainsi en est-il :

- ⇨ de la présence de traces graisseuses sur l'enveloppe ou l'emballage,
- ⇨ de la présence de fil de fer ou de feuilles d'étain si l'enveloppe ou le colis sont endommagés,
- ⇨ d'une odeur de massepain ou d'amande émanant de l'enveloppe ou du colis,
- ⇨ d'une répartition inégale du poids à l'intérieur de l'enveloppe. (Notons qu'une enveloppe ordinaire ne peut être que très difficilement piégée. La plupart du temps les engins explosifs et les systèmes de mise à feu nécessitent l'emploi d'enveloppes renforcées).

On prendra garde de même aux inscriptions manuscrites, dactylographiées ou portant une orthographe défaillante lorsque le colis ou la lettre provient d'un endroit inattendu.

La plus grande attention doit être portée aux missives et colis remis par coursier et provenant d'une source inconnue et peu vérifiable.

C.- Les lettres ou colis suspects pouvant contenir des substances biologiques ou chimiques

Les principes de précaution concernant les lettres ou colis suspects pouvant contenir des substances explosives ou incendiaires sont à appliquer strictement dans ce domaine notamment en ce qui concerne l'établissement d'un périmètre de sécurité adapté à la configuration du lieu de découverte et d'interdiction de manipuler l'objet en cause.

Les points suivants méritent d'être précisés :

1. **En ce qui concerne l'objet :**

- ⇨ laisser l'objet en l'état sans le manipuler ou le changer de lieu,
- ⇨ stopper toute ventilation ou climatisation dans les locaux concernés,
- ⇨ condamner la ou les pièces après avoir fermé les fenêtres pour éviter les circulations d'air, installer une signalétique adaptée, et en interdire strictement l'accès,
- ⇨ recueillir une description précise de l'objet incriminé (pli ouvert ou fermé, taille, couleur, présence d'un timbre ou non, origine administrative ou non, oblitération éventuelle, ainsi que du mode par lequel l'objet s'est trouvé dans le local : courrier normal, pli déposé par porteur ou abandonné sur place par un visiteur.

2. En ce qui concerne les personnes exposées ou susceptibles d'avoir été exposées :

- écarter les personnes ayant été en contact avec l'objet ou la substance,
- les isoler des autres personnes en attente des services de secours dont les personnels sont seuls habilités à les prendre en compte,
- dresser une liste des personnes ayant été en contact direct avec la substance et des personnes se trouvant à proximité mais n'ayant ni respiré ni touché la substance, ces deux types de population faisant par la suite l'objet d'un traitement distinct de la part des services spécialisés.

Remarque : il est recommandé :

- d'équiper les personnels traitant habituellement le courrier avec des gants latex de type chirurgical (ou mieux - utiliser un poche spéciale en plastique transparent avec gants permettant de confiner pour manipuler) afin d'éviter tout contact cutané direct avec le produit,
- de renoncer à l'utilisation de machines automatisées d'ouverture du courrier afin d'éviter la dispersion d'un produit ou d'une substance,
- de s'équiper de dispositifs permettant une ouverture du courrier en atmosphère confinée (courrier douteux mais non suspect).

Seuls les services compétents sont habilités à la mise en sécurité de l'objet suspect et au prélèvement qui pourrait être effectué en cas de nécessité.

Caméra réseau de la gamme AXIS P33 — Modèles d'extérieur

Dômes fixes pour tout environnement avec mise au point et zoom à distance.

- > Qualité d'image exceptionnelle HDTV allant jusqu'à 5 MP
- > WDR avec capture dynamique et Technologie Lightfinder
- > Éclairage infrarouge intégré
- > Mise au point et zoom à distance
- > Contrôle P-Iris
- > Résistance au choc IK10 et modèles pour l'extérieur

Les caméras réseau AXIS P33 constituent une gamme de caméras à dôme fixes adaptée à une utilisation en intérieur comme en extérieur. Ces caméras constituent le meilleur choix pour une vidéo surveillance discrète, de jour comme de nuit, dans des zones exposées telles que la surveillance des zones urbaines, les aéroports, les stations de métro, les commerces de détails, les bâtiments administratifs, les écoles et les campus universitaires.

La gamme AXIS P33 offre une qualité d'image exceptionnelle allant de la résolution SVGA jusqu'à 5 mégapixels, comprenant la vidéo HDTV 720p et 1080p conforme à la norme SMPTE. La gamme AXIS P33 offre de multiples flux de données vidéo H.264 et Motion JPEG configurables individuellement.

Les modèles SVGA et HDTV 720p/1MP prennent en charge la technologie Lightfinder d'Axis, ce qui rend ces cameras extrêmement sensibles aux faibles éclairages. Le modèle AXIS P3384-VE prenant en charge la gamme dynamique étendue (WDR) avec 'capture dynamique', offre une qualité vidéo exceptionnelle dans des conditions extrêmes avec de nombreuses variations de lumière. Le modèle 5 mégapixels, AXIS P3367-VE, peut couvrir une large zone avec des détails exceptionnels et une excellente sensibilité à la lumière. Tous les modèles AXIS P33 prennent en charge le contrôle P-iris pour une clarté optimale de l'image.

AXIS P3364-LVE intègre la nouvelle technologie LED longue durée de vie, très économe en énergie. Avec un angle et une intensité réglables, la solution infrarouge intégrée se configure facilement afin d'être optimisée pour la scène. Toutes les caméras AXIS P33 prennent en charge la fonction de mise au point à distance qui supprime la mise au point manuelle au niveau de la caméra et le zoom à distance qui permet d'optimiser l'angle de vue de la caméra.

Toutes les caméras de la série AXIS P33 sont dotées des fonctions panoramique/inclinaison/zoom et les modèles avec mode de capture à 3 mégapixels et à 5 mégapixels permettent la fonction de flux à vue multiple. Les caméras AXIS P33-VE/-LVE résistantes aux intempéries ont une faible consommation électrique, respectueuse de l'environnement, alimentée par le Power over Ethernet standard (IEEE 802.3af) et fonctionnent à des températures allant de -40 °C à 55 °C.

Des dômes fixes conçus pour une installation efficace

Les modèles d'extérieur de la gamme AXIS P33 constituent le choix idéal pour une large gamme d'applications vidéo exigeantes. Les caméras réseau AXIS P33 ont été conçues pour une surveillance vidéo professionnelle, avec une installation et une mise au point simple et fiable.

Installation prévue en extérieur, dans des conditions climatiques extrêmes

Les modèles de la gamme AXIS P33 destinés à un fonctionnement en extérieur sont spécialement conçus pour une installation fiable, anti-vandale et résistantes aux intempéries, avec un système préinstallé de chauffage et de ventilation ainsi qu'une membrane de déshumidification supprimant toute humidité infiltrée dans le boîtier de la caméra pendant l'installation. Ces caméras sont livrées avec un câble Ethernet de 5 m (16 pi), et équipées d'un joint pré-monté spécialement conçu pour permettre une installation à même le mur sans nécessiter d'isolant supplémentaire. La protection étanche incluse assure une protection efficace contre les réflexions de la lumière solaire ou les accumulations d'eau de pluie ou de neige, sauf pour le modèle AXIS P3364-LVE, pour lequel la protection étanche pourrait interférer avec l'éclairage infrarouge intégré. Une gamme variée de kits de montage facultatifs est disponible, par exemple pour le montage sur un mur, un poteau ou un support d'angle.

Technologie Lightfinder

Les modèles SVGA et HDTV 720p/1MP de la gamme AXIS P33 intègrent le Lightfinder, une technologie unique d'Axis. Leur remarquable sensibilité à la lumière, avec le maintien des couleurs même dans des conditions de faible éclairage, est obtenue en associant l'expertise d'Axis dans le traitement des images, le développement des systèmes sur puce et une sélection des meilleurs composants optiques.
Pour plus d'informations sur la technologie Lightfinder, rendez-vous sur :
www.axis.com/corporate/corp/tech_papers.htm

La capture dynamique – WDR

Le modèle AXIS P3384-VE prenant en charge le WDR avec 'capture dynamique' est idéal pour la surveillance de zones avec de fortes variations de lumière, par exemple dans les tunnels ou d'autres zones où la lumière du soleil crée aussi bien des zones très éclairées et que des ombres foncées. Le modèle AXIS P3384-VE permet une identification simple et claire des personnes et des objets dans des zones éclairées et sombres.

Éclairage infrarouge intégré

Le modèle AXIS P3364-LVE se caractérise par un éclairage infrarouge intégré basé sur la nouvelle technologie LED ayant une longue durée de vie qui est très économe en énergie. Cela se traduit par une vidéo de haute qualité, à faible bruit même lorsque l'environnement est complètement noir.

Contrôle P-Iris

La gamme P33 intègre un nouveau contrôle précis et avancé de l'iris grâce à un objectif P-Iris spécial associé à un logiciel dédié dans la caméra qui définit la meilleure position de l'iris pour une profondeur de champ, une résolution, un contraste de l'image et une clarté optimaux. Une bonne profondeur de champ implique que les objets situés à différentes distances de la caméra soient mis au point simultanément.
Pour en savoir plus sur le P-Iris et le contrôle de l'iris, cliquez sur le lien :
www.axis.com/corporate/corp/tech_papers.htm

Installation simple

Les caméras réseau AXIS P33 offrent des possibilités d'installations uniques, avec mise au point et zoom à distance. La fonctionnalité de mise au point à distance permet un réglage facile de la mise au point à travers le réseau, ce qui évite d'avoir à régler la caméra manuellement. Grâce à la fonctionnalité de zoom à distance, l'angle de vue de la caméra est optimisé pour la zone à surveiller. Le compteur de pixels permet de garantir une résolution parfaite des pixels. La solution infrarouge intégrée dans l'AXIS P3364-LVE adapte automatiquement l'angle d'éclairage avec le niveau de zoom, ce qui simplifie l'installation.

Caractéristiques techniques – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

Caméra

Modèles d'extérieur	**AXIS P3363-VE :** SVGA, Lightfinder **AXIS P3364-VE :** 1 MP, Lightfinder **AXIS P3364-LVE : 1** MP, Éclairage infrarouge, Lightfinder **AXIS P3384-VE :** 1 MP, WDR - capture dynamique, Lightfinder **AXIS P3346-VE :** 3 MP, flux à vue multiple **AXIS P3367-VE :** 5 MP, flux à vue multiple *Remarque : Tous les modèles sont anti-vandalisme et prennent en charge l'audio et les ports E/S* *6 mm et 12 mm en tant que suffixe font référence au modèle de l'objectif*
Capteur d'image	**AXIS P3363-VE :** Capteur CMOS RGB à balayage progressif 1/3" **AXIS P3364-VE/-LVE :** Capteur CMOS RGB à balayage progressif 1/3" **AXIS P3384-VE :** Capteur CMOS RGB à balayage progressif 1/3" **AXIS P3346-VE :** Capteur CMOS RGB à balayage progressif 1/3" (effectif) **AXIS P3367-VE :** Capteur CMOS RGB à balayage progressif 1/3,2"
Objectif	Foyer progressif, mise au point et zoom à distance, contrôle P-Iris, correction infrarouge, résolution des mégapixels **AXIS P3363-VE/P3364-VE 6 mm :** 2,5-6 mm, vue 105° - 49°*, F1,2 **AXIS P3363-VE/P3364-VE/P3364-LVE 12 mm :** 3,3-12 mm, vue 82° - 24°*, F1,4 **AXIS P3384-VE :** 3-9 mm, vue 84° - 30°*, F1,2 **AXIS P3346-VE :** 3-9 mm, vue 84° - 30°*, F1,2 **AXIS P3367-VE :** 3-9 mm, vue 84° - 30°*, F1,2 *angle de vue horizontal
De jour comme de nuit	Filtre de coupure infrarouge amovible automatiquement
Éclairage minimum	**AXIS P3363-VE/P3364-VE 6 mm :** Couleur : 0,1 lux, F1,2, N/B : 0,02 lux, F1,2 **AXIS P3363-VE/P3364-VE 12 mm :** Couleur : 0,15 lux, F1,4, N/B : 0,03 lux, F1,4 **AXIS P3364-LVE 12 mm :** Couleur : 0,18 lux, F1,4, N/B : 0,04 lux, 0 lux avec éclairage infrarouge activé **AXIS P3384-VE :** Couleur : 0,5 lux, F1,2, N/B : 0,08 lux, F1,2 avec capture dynamique Couleur : 0,15 lux, F1,2, N/B : 0,03 lux, F1,2 avec Lightfinder **AXIS P3346-VE : Couleur :** 0,5 lux, F1,2, N/B : 0,08 lux, F1,2 **AXIS P3367-VE : Couleur :** 0,2 lux, N/B : 0,04 lux, F1,2
Vitesse d'obturation	**AXIS P3363-VE/P3364-VE/P3364-LVE :** 1/24500 s à 2 s avec une fréquence du réseau de 50 Hz, 1/29500 s à 2 s avec une fréquence du réseau de 60 Hz **AXIS P3384-VE :** Capture dynamique : 1/192 s à 1/37 s avec une fréquence du réseau de 50 Hz, 1/231 s à 1/44 s avec une fréquence du réseau de 60 Hz ; Lightfinder : 1/24500 s à 2 s avec une fréquence du réseau de 50 Hz 1/29500 s à 2 s avec une fréquence du réseau de 60 Hz **AXIS P3346-VE :** 1/35500 s à 1/6 s **AXIS P3367-VE :** 1/28000 s à 2 s
Réglage de l'angle de la caméra	**AXIS P3363-VE/P3364-VE/P3364-LVE :** Panoramique 360°, inclinaison 170°, rotation 340° **AXIS P3384-VE/P3346-VE/P3367-VE :** Panoramique 360°, inclinaison 160°, rotation 340°

Vidéo

Compression vidéo	Profil de base et profil principal H.264 (MPEG-4 partie 10/AVC) Motion JPEG
Résolutions	**AXIS P3363-VE :** 800x600 (SVGA) à 160x90 **AXIS P3364-VE/P3364-LVE/P3384-VE :** 1280x960* (approx. 1,3 MP) à 160x90 **AXIS P3346-VE :** 2048x1536 (3 MP) à 160x90 **AXIS P3367-VE :** 2592x1944 (5 mégapixels) à 160x90 *1400x1050 (1,4 MP) résolution proportionnée disponible via VAPIX®
Fréquence d'images H.264/ Motion JPEG	**AXIS P3363-VE/P3364-VE/P3364-LVE/P3384-VE :** 25 ips avec fréquence du réseau de 50 Hz, 30 ips avec fréquence du réseau de 60 Hz **AXIS P3346-VE :** Mode de capture 3 mégapixels : 20 ips dans toutes les résolutions ; modes de capture HDTV 1080p (1920x1080) et 2 MP 4:3 (1600x1200) : 30 ips dans toutes les résolutions **AXIS P3367-VE :** Mode de capture 5 mégapixels : 12 ips dans toutes les résolutions ; et compatible avec tous les modes de capture AXIS P3346-VE
Flux vidéo	Flux H.264 et Motion JPEG multiples configurables individuellement Fréquence d'image et bande passante contrôlables VBR/CBR H.264
Flux à vue multiple	**AXIS P3346-VE/P3367-VE :** Jusqu'à 8 zones détourées de la vue individuellement **AXIS P3346-VE :** Lors de la diffusion de zones à 4 vues et d'une vue d'ensemble en résolution VGA, la fréquence d'images est de 20 ips par flux (mode de capture 3 MP) **AXIS P3367-VE :** Lors de la diffusion de zones à 4 vues et d'une vue d'ensemble en résolution VGA, la fréquence d'images est de 12 ips par flux (mode de capture 5 MP) ou de 20 ips par flux (mode de capture 3 MP)
Panoramique/ Inclinaison/Zoom	PTZ numérique, positions préréglées et tour de garde
Réglages de l'image	Compression, couleur, luminosité, netteté, contraste, balance des blancs, contrôle d'exposition, zones d'exposition, compensation du rétroéclairage, gamme dynamique étendue (WDR) - contraste dynamique, ajustement de précision en cas de faible éclairage Rotation : 0°, 90°, 180°, 270°, incluant le format corridor Surimpression de texte et d'images, masque de confidentialité, duplication des images **AXIS P3384-VE :** WDR - Capture dynamique : Jusqu'à 120 dB (0,5 – 500 000 lux) en fonction de la scène

Audio

Flux audio	Bidirectionnelle
Compression audio	AAC LC 8/16 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz Débit binaire configurable
Entrée/sortie audio	Entrée/sortie de microphone externe

Réseaux

Sécurité	Protection par mot de passe, filtrage d'adresses IP, authentification Digest, journal des accès utilisateurs, contrôle d'accès aux réseaux IEEE 802.1X**, cryptage HTTPS**
Protocoles pris en charge	IPv4/v6, HTTP, HTTPS**, SSL/TLS**, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS

Intégration système

Interface de programmation d'applications	API ouverte pour l'intégration logicielle, comprenant les caractéristiques ONVIF disponibles sur www.onvif.org, ainsi que VAPIX® et la plateforme d'applications pour caméras AXIS d'Axis Communications, caractéristiques disponibles sur le site www.axis.com Prise en charge du système d'hébergement vidéo AXIS (AVHS) avec connexion de la caméra en un seul clic connexion
Vidéo intelligente	Détection de mouvement vidéo, alarme anti-sabotage active, détection audio Prise en charge la plate-forme d'applications pour caméras AXIS permettant l'installation d'applications supplémentaires
Déclencheurs d'événements	Vidéo intelligente, entrée externe, évènements de stockage edge
Actions d'événements	Téléchargement de fichiers : FTP, HTTP, partage de réseau et courrier électronique Notification : courrier électronique, HTTP et TCP Activation de la sortie externe Enregistrement vidéo et audio vers un stockage edge Mise en mémoire tampon vidéo pré/post-alarme Lecture de clip audio PTZ préréglé, tour de garde **AXIS P3364-LVE :** Activation de l'éclairage infrarouge
Flux de données	Données d'évènements
Aides à l'installation intégrées	Zoom à distance, mise au point à distance et compteur de pixels **AXIS P3364-LVE :** angle et intensité de l'éclairage infrarouge réglable

***Ce produit inclut un logiciel développé par le projet OpenSSL pour une utilisation avec la boîte à outils OpenSSL. (www.openssl.org)*

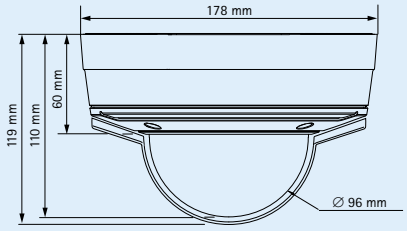
Caractéristiques techniques (suite) – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

Général	
Boîtier	Couvercle transparent en polycarbonate Module interne de caméra en aluminium avec composants électroniques encapsulés Couleur : Blanc NCS S 1002-B Boîtier en aluminium IK10 résistant aux chocs avec membrane déshumidifiante intégrée, certifié IP66 et NEMA 4X
Mémoire	256 Mo de mémoire RAM, 128 Mo de mémoire Flash **AXIS P3367-VE :** 512 Mo de mémoire RAM, 128 Mo de mémoire Flash
Alimentation	Power over Ethernet IEEE 802.3af **AXIS P3363-VE/P3364-VE/P3364-LVE/P3384-VE/P3367-VE :** Classe 3 ; 12.1 W max **AXIS P3346-VE :** Classe 3 ; 12,8 W max
Connecteurs	RJ45 10BASE-T/100BASE-TX PoE Plaque à bornes pour 1 entrée d'alarme et 1 sortie Entrée de ligne/micro 3,5 mm, sortie de ligne 3,5 mm
Éclairage infrarouge	**AXIS P3364-LVE :** Économes en énergie, LED infrarouge ayant une longue durée de vie avec angle et intensité d'éclairage réglables. Plage allant jusqu'à 30 m en fonction de la scène
Stockage edge	Port SD/SDHC/SDXC pour carte mémoire jusqu'à 64 GB (carte non fournie) Prise en charge de l'enregistrement vers un stockage réseau partagé (NAS ou serveurs de fichiers)
Conditions d'utilisation	-40 °C á 55 °C Humidité relative de 10 à 100 % (condensation)
Homologations	EN 50121-4, EN 55022, EN 55024, EN 61000-6-1, EN 61000-6-2, IEC/EN/UL 60950-1, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-64, IEC 60068-2-78, IEC 60529 IP66, NEMA 250 Type 4X, IEC 62236-4, IEC 62262 IK10, FCC Partie 15, Sous-partie B Classe B, ICES-003 Classe B numérique, VCCI, ITE, C-tick AS/NZS CISPR 22, KCC AS/NZS CISPR 22, KN 22, KN 24 **AXIS P3364-LVE :** EN 62471
Accessoires inclus	Guide d'installation, CD du logiciel d'installation et de gestion, Licence pour 1 utilisateur du logiciel de décodage Windows, kit du connecteur, support de montage, câble réseau de 5 m avec joint pré-monté **AXIS P3363-VE/P3364-VE/P3384-VE/P3346-VE/P3367-VE :** Protection étanche, couvercle fumé transparent

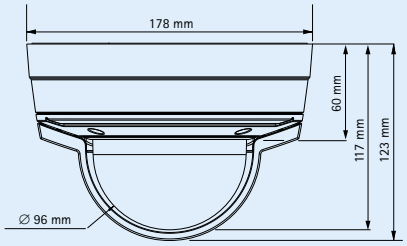
Pour plus d'informations, visitez le site www.axis.com

Dimensions et poids – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

AXIS P3363-VE, P3364-VE
Poids : 1,5 kg, avec protection étanche
AXIS P3364-LVE:
Poids : 1,4 kg, protection étanche non comprise



AXIS P3384-VE, AXIS P3346-VE, AXIS P3367-VE
Poids : 1,7 kg, avec protection étanche



Accessoires – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

Accessoires optionnels pour les modèles destinés à l'extérieur

Kit de suspension avec protection étanche

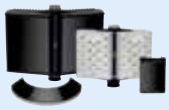
Supports AXIS T91A

Mur

Support d'angle

Câble audio E/S, 5 m

Projecteurs Axis



Protection pour câbles, incluant l'adaptateur NPS de 3/4" pouce pour AXIS P33-VE

Logiciel de gestion vidéo

AXIS Camera Companion (inclus), AXIS Camera Station et le logiciel de gestion vidéo des Partenaires de Développement d'Application Axis (non inclus).
Pour plus d'information, rendez-vous sur www.axis.com/products/video/software

Axis Communications SAS - RCS B408969998 49391/FR/R1/1303

Caméra réseau de la gamme AXIS P33 — Modèles d'extérieur

Dômes fixes pour tout environnement avec mise au point et zoom à distance.

- > Qualité d'image exceptionnelle HDTV allant jusqu'à 5 MP
- > WDR avec capture dynamique et Technologie Lightfinder
- > Éclairage infrarouge intégré
- > Mise au point et zoom à distance
- > Contrôle P-Iris
- > Résistance au choc IK10 et modèles pour l'extérieur

Les caméras réseau AXIS P33 constituent une gamme de caméras à dôme fixes adaptée à une utilisation en intérieur comme en extérieur. Ces caméras constituent le meilleur choix pour une vidéo surveillance discrète, de jour comme de nuit, dans des zones exposées telles que la surveillance des zones urbaines, les aéroports, les stations de métro, les commerces de détails, les bâtiments administratifs, les écoles et les campus universitaires.

La gamme AXIS P33 offre une qualité d'image exceptionnelle allant de la résolution SVGA jusqu'à 5 mégapixels, comprenant la vidéo HDTV 720p et 1080p conforme à la norme SMPTE. La gamme AXIS P33 offre de multiples flux de données vidéo H.264 et Motion JPEG configurables individuellement.

Les modèles SVGA et HDTV 720p/1MP prennent en charge la technologie Lightfinder d'Axis, ce qui rend ces cameras extrêmement sensibles aux faibles éclairages. Le modèle AXIS P3384-VE prenant en charge la gamme dynamique étendue (WDR) avec 'capture dynamique', offre une qualité vidéo exceptionnelle dans des conditions extrêmes avec de nombreuses variations de lumière. Le modèle 5 mégapixels, AXIS P3367-VE, peut couvrir une large zone avec des détails exceptionnels et une excellente sensibilité à la lumière. Tous les modèles AXIS P33 prennent en charge le contrôle P-iris pour une clarté optimale de l'image.

AXIS P3364-LVE intègre la nouvelle technologie LED longue durée de vie, très économe en énergie. Avec un angle et une intensité réglables, la solution infrarouge intégrée se configure facilement afin d'être optimisée pour la scène. Toutes les caméras AXIS P33 prennent en charge la fonction de mise au point à distance qui supprime la mise au point manuelle au niveau de la caméra et le zoom à distance qui permet d'optimiser l'angle de vue de la caméra.

Toutes les caméras de la série AXIS P33 sont dotées des fonctions panoramique/inclinaison/zoom et les modèles avec mode de capture à 3 mégapixels et à 5 mégapixels permettent la fonction de flux à vue multiple. Les caméras AXIS P33-VE/-LVE résistantes aux intempéries ont une faible consommation électrique, respectueuse de l'environnement, alimentée par le Power over Ethernet standard (IEEE 802.3af) et fonctionnent à des températures allant de -40 °C à 55 °C.

Des dômes fixes conçus pour une installation efficace

Les modèles d'extérieur de la gamme AXIS P33 constituent le choix idéal pour une large gamme d'applications vidéo exigeantes. Les caméras réseau AXIS P33 ont été conçues pour une surveillance vidéo professionnelle, avec une installation et une mise au point simple et fiable.

Installation prévue en extérieur, dans des conditions climatiques extrêmes

Les modèles de la gamme AXIS P33 destinés à un fonctionnement en extérieur sont spécialement conçus pour une installation fiable, anti-vandale et résistantes aux intempéries, avec un système préinstallé de chauffage et de ventilation ainsi qu'une membrane de déshumidification supprimant toute humidité infiltrée dans le boîtier de la caméra pendant l'installation. Ces caméras sont livrées avec un câble Ethernet de 5 m (16 pi), et équipées d'un joint pré-monté spécialement conçu pour permettre une installation à même le mur sans nécessiter d'isolant supplémentaire. La protection étanche incluse assure une protection efficace contre les réflexions de la lumière solaire ou les accumulations d'eau de pluie ou de neige, sauf pour le modèle AXIS P3364-LVE, pour lequel la protection étanche pourrait interférer avec l'éclairage infrarouge intégré. Une gamme variée de kits de montage facultatifs est disponible, par exemple pour le montage sur un mur, un poteau ou un support d'angle.

Technologie Lightfinder

Les modèles SVGA et HDTV 720p/1MP de la gamme AXIS P33 intègrent le Lightfinder, une technologie unique d'Axis. Leur remarquable sensibilité à la lumière, avec le maintien des couleurs même dans des conditions de faible éclairage, est obtenue en associant l'expertise d'Axis dans le traitement des images, le développement des systèmes sur puce et une sélection des meilleurs composants optiques.
Pour plus d'informations sur la technologie Lightfinder, rendez-vous sur :
www.axis.com/corporate/corp/tech_papers.htm

La capture dynamique – WDR

Le modèle AXIS P3384-VE prenant en charge le WDR avec 'capture dynamique' est idéal pour la surveillance de zones avec de fortes variations de lumière, par exemple dans les tunnels ou d'autres zones où la lumière du soleil crée aussi bien des zones très éclairées et que des ombres foncées. Le modèle AXIS P3384-VE permet une identification simple et claire des personnes et des objets dans des zones éclairées et sombres.

Éclairage infrarouge intégré

Le modèle AXIS P3364-LVE se caractérise par un éclairage infrarouge intégré basé sur la nouvelle technologie LED ayant une longue durée de vie qui est très économe en énergie. Cela se traduit par une vidéo de haute qualité, à faible bruit même lorsque l'environnement est complètement noir.

Contrôle P-Iris

La gamme P33 intègre un nouveau contrôle précis et avancé de l'iris grâce à un objectif P-Iris spécial associé à un logiciel dédié dans la caméra qui définit la meilleure position de l'iris pour une profondeur de champ, une résolution, un contraste de l'image et une clarté optimaux. Une bonne profondeur de champ implique que les objets situés à différentes distances de la caméra soient mis au point simultanément.
Pour en savoir plus sur le P-Iris et le contrôle de l'iris, cliquez sur le lien :
www.axis.com/corporate/corp/tech_papers.htm

Installation simple

Les caméras réseau AXIS P33 offrent des possibilités d'installations uniques, avec mise au point et zoom à distance. La fonctionnalité de mise au point à distance permet un réglage facile de la mise au point à travers le réseau, ce qui évite d'avoir à régler la caméra manuellement. Grâce à la fonctionnalité de zoom à distance, l'angle de vue de la caméra est optimisé pour la zone à surveiller. Le compteur de pixels permet de garantir une résolution parfaite des pixels. La solution infrarouge intégrée dans l'AXIS P3364-LVE adapte automatiquement l'angle d'éclairage avec le niveau de zoom, ce qui simplifie l'installation.

Caractéristiques techniques – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

Caméra

Modèles d'extérieur	**AXIS P3363-VE :** SVGA, Lightfinder **AXIS P3364-VE :** 1 MP, Lightfinder **AXIS P3364-LVE : 1** MP, Éclairage infrarouge, Lightfinder **AXIS P3384-VE :** 1 MP, WDR - capture dynamique, Lightfinder **AXIS P3346-VE :** 3 MP, flux à vue multiple **AXIS P3367-VE :** 5 MP, flux à vue multiple *Remarque : Tous les modèles sont anti-vandalisme et prennent en charge l'audio et les ports E/S* *6 mm et 12 mm en tant que suffixe font référence au modèle de l'objectif*
Capteur d'image	**AXIS P3363-VE :** Capteur CMOS RGB à balayage progressif 1/3" **AXIS P3364-VE/-LVE :** Capteur CMOS RGB à balayage progressif 1/3" **AXIS P3384-VE :** Capteur CMOS RGB à balayage progressif 1/3" **AXIS P3346-VE :** Capteur CMOS RGB à balayage progressif 1/3" (effectif) **AXIS P3367-VE :** Capteur CMOS RGB à balayage progressif 1/3,2"
Objectif	Foyer progressif, mise au point et zoom à distance, contrôle P-Iris, correction infrarouge, résolution des mégapixels **AXIS P3363-VE/P3364-VE 6 mm :** 2,5-6 mm, vue 105° - 49°*, F1,2 **AXIS P3363-VE/P3364-VE/P3364-LVE 12 mm :** 3,3-12 mm, vue 82° - 24°*, F1,4 **AXIS P3384-VE :** 3-9 mm, vue 84° - 30°*, F1,2 **AXIS P3346-VE :** 3-9 mm, vue 84° - 30°*, F1,2 **AXIS P3367-VE :** 3-9 mm, vue 84° - 30°*, F1,2 *angle de vue horizontal
De jour comme de nuit	Filtre de coupure infrarouge amovible automatiquement
Éclairage minimum	**AXIS P3363-VE/P3364-VE 6 mm :** Couleur : 0,1 lux, F1,2, N/B : 0,02 lux, F1,2 **AXIS P3363-VE/P3364-VE 12 mm :** Couleur : 0,15 lux, F1,4, N/B : 0,03 lux, F1,4 **AXIS P3364-LVE 12 mm :** Couleur : 0,18 lux, F1,4, N/B : 0,04 lux, 0 lux avec éclairage infrarouge activé **AXIS P3384-VE :** Couleur : 0,5 lux, F1,2, N/B : 0,08 lux, F1,2 avec capture dynamique Couleur : 0,15 lux, F1,2, N/B : 0,03 lux, F1,2 avec Lightfinder **AXIS P3346-VE : Couleur :** 0,5 lux, F1,2, N/B : 0,08 lux, F1,2 **AXIS P3367-VE : Couleur :** 0,2 lux, N/B : 0,04 lux, F1,2
Vitesse d'obturation	**AXIS P3363-VE/P3364-VE/P3364-LVE :** 1/24500 s à 2 s avec une fréquence du réseau de 50 Hz, 1/29500 s à 2 s avec une fréquence du réseau de 60 Hz **AXIS P3384-VE :** Capture dynamique : 1/192 s à 1/37 s avec une fréquence du réseau de 50 Hz, 1/231 s à 1/44 s avec une fréquence du réseau de 60 Hz ; Lightfinder : 1/24500 s à 2 s avec une fréquence du réseau de 50 Hz 1/29500 s à 2 s avec une fréquence du réseau de 60 Hz **AXIS P3346-VE :** 1/35500 s à 1/6 s **AXIS P3367-VE :** 1/28000 s à 2 s
Réglage de l'angle de la caméra	**AXIS P3363-VE/P3364-VE/P3364-LVE :** Panoramique 360°, inclinaison 170°, rotation 340° **AXIS P3384-VE/P3346-VE/P3367-VE :** Panoramique 360°, inclinaison 160°, rotation 340°

Vidéo

Compression vidéo	Profil de base et profil principal H.264 (MPEG-4 partie 10/AVC) Motion JPEG
Résolutions	**AXIS P3363-VE :** 800x600 (SVGA) à 160x90 **AXIS P3364-VE/P3364-LVE/P3384-VE :** 1280x960* (approx. 1,3 MP) à 160x90 **AXIS P3346-VE :** 2048x1536 (3 MP) à 160x90 **AXIS P3367-VE :** 2592x1944 (5 mégapixels) à 160x90 *1400x1050 (1,4 MP) résolution proportionnée disponible via VAPIX®
Fréquence d'images H.264/ Motion JPEG	**AXIS P3363-VE/P3364-VE/P3364-LVE/P3384-VE :** 25 ips avec fréquence du réseau de 50 Hz, 30 ips avec fréquence du réseau de 60 Hz **AXIS P3346-VE :** Mode de capture 3 mégapixels : 20 ips dans toutes les résolutions ; modes de capture HDTV 1080p (1920x1080) et 2 MP 4:3 (1600x1200) : 30 ips dans toutes les résolutions **AXIS P3367-VE :** Mode de capture 5 mégapixels : 12 ips dans toutes les résolutions ; et compatible avec tous les modes de capture AXIS P3346-VE
Flux vidéo	Flux H.264 et Motion JPEG multiples configurables individuellement Fréquence d'image et bande passante contrôlables VBR/CBR H.264
Flux à vue multiple	**AXIS P3346-VE/P3367-VE :** Jusqu'à 8 zones détourées de la vue individuellement **AXIS P3346-VE :** Lors de la diffusion de zones à 4 vues et d'une vue d'ensemble en résolution VGA, la fréquence d'images est de 20 ips par flux (mode de capture 3 MP) **AXIS P3367-VE :** Lors de la diffusion de zones à 4 vues et d'une vue d'ensemble en résolution VGA, la fréquence d'images est de 12 ips par flux (mode de capture 5 MP) ou de 20 ips par flux (mode de capture 3 MP)
Panoramique/ Inclinaison/Zoom	PTZ numérique, positions préréglées et tour de garde
Réglages de l'image	Compression, couleur, luminosité, netteté, contraste, balance des blancs, contrôle d'exposition, zones d'exposition, compensation du rétroéclairage, gamme dynamique étendue (WDR) - contraste dynamique, ajustement de précision en cas de faible éclairage Rotation : 0°, 90°, 180°, 270°, incluant le format corridor Surimpression de texte et d'images, masque de confidentialité, duplication des images **AXIS P3384-VE :** WDR - Capture dynamique : Jusqu'à 120 dB (0,5 – 500 000 lux) en fonction de la scène

Audio

Flux audio	Bidirectionnelle
Compression audio	AAC LC 8/16 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz Débit binaire configurable
Entrée/sortie audio	Entrée/sortie de microphone externe

Réseaux

Sécurité	Protection par mot de passe, filtrage d'adresses IP, authentification Digest, journal des accès utilisateurs, contrôle d'accès aux réseaux IEEE 802.1X**, cryptage HTTPS**
Protocoles pris en charge	IPv4/v6, HTTP, HTTPS**, SSL/TLS**, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS

Intégration système

Interface de programmation d'applications	API ouverte pour l'intégration logicielle, comprenant les caractéristiques ONVIF disponibles sur www.onvif.org, ainsi que VAPIX® et la plateforme d'applications pour caméras AXIS d'Axis Communications, caractéristiques disponibles sur le site www.axis.com Prise en charge du système d'hébergement vidéo AXIS (AVHS) avec connexion de la caméra en un seul clic connexion
Vidéo intelligente	Détection de mouvement vidéo, alarme anti-sabotage active, détection audio Prise en charge la plate-forme d'applications pour caméras AXIS permettant l'installation d'applications supplémentaires
Déclencheurs d'événements	Vidéo intelligente, entrée externe, évènements de stockage edge
Actions d'événements	Téléchargement de fichiers : FTP, HTTP, partage de réseau et courrier électronique Notification : courrier électronique, HTTP et TCP Activation de la sortie externe Enregistrement vidéo et audio vers un stockage edge Mise en mémoire tampon vidéo pré/post-alarme Lecture de clip audio PTZ préréglé, tour de garde **AXIS P3364-LVE :** Activation de l'éclairage infrarouge
Flux de données	Données d'évènements
Aides à l'installation intégrées	Zoom à distance, mise au point à distance et compteur de pixels **AXIS P3364-LVE :** angle et intensité de l'éclairage infrarouge réglable

***Ce produit inclut un logiciel développé par le projet OpenSSL pour une utilisation avec la boîte à outils OpenSSL. (www.openssl.org)*

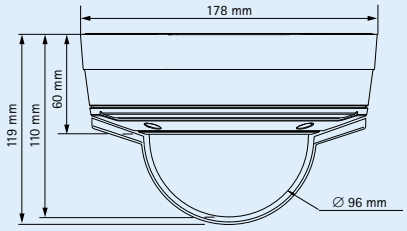
Caractéristiques techniques (suite) – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

Général	
Boîtier	Couvercle transparent en polycarbonate Module interne de caméra en aluminium avec composants électroniques encapsulés Couleur : Blanc NCS S 1002-B Boîtier en aluminium IK10 résistant aux chocs avec membrane déshumidifiante intégrée, certifié IP66 et NEMA 4X
Mémoire	256 Mo de mémoire RAM, 128 Mo de mémoire Flash **AXIS P3367-VE :** 512 Mo de mémoire RAM, 128 Mo de mémoire Flash
Alimentation	Power over Ethernet IEEE 802.3af **AXIS P3363-VE/P3364-VE/P3364-LVE/P3384-VE/P3367-VE :** Classe 3 ; 12.1 W max **AXIS P3346-VE :** Classe 3 ; 12,8 W max
Connecteurs	RJ45 10BASE-T/100BASE-TX PoE Plaque à bornes pour 1 entrée d'alarme et 1 sortie Entrée de ligne/micro 3,5 mm, sortie de ligne 3,5 mm
Éclairage infrarouge	**AXIS P3364-LVE :** Économes en énergie, LED infrarouge ayant une longue durée de vie avec angle et intensité d'éclairage réglables. Plage allant jusqu'à 30 m en fonction de la scène
Stockage edge	Port SD/SDHC/SDXC pour carte mémoire jusqu'à 64 GB (carte non fournie) Prise en charge de l'enregistrement vers un stockage réseau partagé (NAS ou serveurs de fichiers)
Conditions d'utilisation	-40 °C á 55 °C Humidité relative de 10 à 100 % (condensation)
Homologations	EN 50121-4, EN 55022, EN 55024, EN 61000-6-1, EN 61000-6-2, IEC/EN/UL 60950-1, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-64, IEC 60068-2-78, IEC 60529 IP66, NEMA 250 Type 4X, IEC 62236-4, IEC 62262 IK10, FCC Partie 15, Sous-partie B Classe B, ICES-003 Classe B numérique, VCCI, ITE, C-tick AS/NZS CISPR 22, KCC AS/NZS CISPR 22, KN 22, KN 24 **AXIS P3364-LVE :** EN 62471
Accessoires inclus	Guide d'installation, CD du logiciel d'installation et de gestion, Licence pour 1 utilisateur du logiciel de décodage Windows, kit du connecteur, support de montage, câble réseau de 5 m avec joint pré-monté **AXIS P3363-VE/P3364-VE/P3384-VE/P3346-VE/P3367-VE :** Protection étanche, couvercle fumé transparent

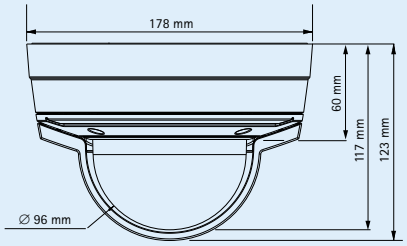
Pour plus d'informations, visitez le site www.axis.com

Dimensions et poids – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

AXIS P3363-VE, P3364-VE
Poids : 1,5 kg, avec protection étanche
AXIS P3364-LVE:
Poids : 1,4 kg, protection étanche non comprise



AXIS P3384-VE, AXIS P3346-VE, AXIS P3367-VE
Poids : 1,7 kg, avec protection étanche



Accessoires – Caméra réseau de la gamme AXIS P33, modèles d'extérieur

Accessoires optionnels pour les modèles destinés à l'extérieur

Kit de suspension avec protection étanche

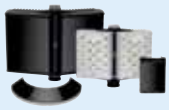
Supports AXIS T91A

Mur

Support d'angle

Câble audio E/S, 5 m

Projecteurs Axis



Protection pour câbles, incluant l'adaptateur NPS de 3/4" pouce pour AXIS P33-VE

Logiciel de gestion vidéo

AXIS Camera Companion (inclus), AXIS Camera Station et le logiciel de gestion vidéo des Partenaires de Développement d'Application Axis (non inclus).
Pour plus d'information, rendez-vous sur www.axis.com/products/video/software

Axis Communications SAS - RCS B408969998 49391/FR/R1/1303

DynaHawk™ X1 Series

Full HD Multiple Streams Ultra-WDR Micro Dome IP Camera

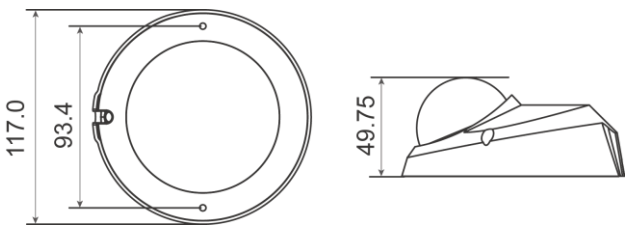
The Full HD Multiple Streams Ultra-WDR Compact Fixed Dome IP Camera offer high definition resolution at full frame rate, progressive scan technology, and edge enhancement for outstanding picture clarity. ONVIF (Profile S) compliance ensures hassle-free, flexible system integration.

This model capable of serving real-time streaming and makes image quality more smoothly. In addition to MJPEG real time streaming, this camera develops H.264 codec to apply for high resolution digital broadcast. With Shutter WDR function, this model can provide better image quality under extreme light contrast scenarios or changing lighting environments.

X1 is a cost-effective surveillance solution for installations that require excellent picture quality at minimal bandwidth. Their simple yet solid, low-profile design is ideal for discreet installations where space is limited. Installation and setup is simple, quick and easy, with a factory-focused lens and a simple PoE connection.

Key Features

- Sony Progressive Scan CMOS Sensor
- 1.3M / 2M Resolution*
- Quad Streams Support
- Dual Streams, Full HD 1080P Real-Time + Full HD 1080P Real-Time
- Quad Stream Compression - H.264 Baseline / Main / High Profile + MJPEG
- Multi-language Support
- Tampering Alarm
- Ultra Dynamic Range
- Motion Detection
- Privacy Masks
- 3D Noise Reduction / 2D Noise Reduction
- Network Failure Detection
- Digital Image Stabilization (DIS)
- Weatherproof Dongle Cable*
- Weatherproof (IP66 International)
- microSD Support
- ONVIF Support



DynaHawk™ X1 Series - Micro Dome IP Camera

Camera		X0S7-1	X0S6-1
Image Sensor		1/2.8" Sony Progressive CMOS	1/3" Sony Progressive CMOS
Effective Pixels		1920(H) x 1080(V)	1280(H) x 1024(V)
Minimum Illumination		0.05 lux (color)	TBD
White Balance		Manual / AWB / ATW	
Shutter Speed		1 ~ 1/10000 sec.	

Lens			
Focal Length		3.6 mm	3.6 mm
F Number		F 1.8	F 1.8
FOV		78°	71.4°

Operation			
Multiple Languages		English / French / German / Italian / Japanese / Korean / Portuguese / Russian / Simplified Chinese / Spanish / Traditional Chinese	
Image Setting	Backlight Compensation	On/Off	
	White Balance	Auto / Manual / ATW	
	Noise Reduction 3D	On/Off	
	Wide Dynamic Range	Shutter WDR (96dB)	Shutter WDR (120dB)
	Privacy Mask	On/Off	
	Brightness	Manual	
	Exposure	Auto / Manual	
	Sharpness	Manual	
	Contrast	Manual	
	Saturation	Manual	
	Hue	Manual	
	Digital Zoom	Support	
	Motion Detection	On / Off / By Schedule	
	Privacy Mask Type	Color	
	Tampering Alarm	On / Off / By Schedule	
	Digital Image Stabiliation	On/Off	
Audio	One-way Audio*	Mic in	
	Compression	G.711/G.726	

Network			
Interface		RJ-45, 10/100/1000 Mbps Ethernet (Giga Ethernet)	
Video Compression		H.264 (MPEG-4 Part 10/AVC) / MJPEG	
Video Streaming	Dual Streams	PAL: H.264 1080P(50 fps) + H.264/MJPEG D1(50 fps)	H.264 720P(50/60 fps) + H.264/MJPEG SVGA(50/60 fps)
	Quad Streams	H.264 1080P(25/30 fps) + H.264 720P(25/30 fps) + H.264 720P(25/30 fps) + H.264/MJPEG CIF(25/30 fps)	H.264 SXGA(25/30 fps) + H.264 720P(25/30 fps) + H.264 SVGA(25/30 fps) + H.264/MJPEG CIF(25/30 fps)
Video Resolution		Full HD 1080P / SXGA / HD 720P / XGA / SVGA / D1 / VGA / CIF / QCIF @50/60fps or 25/30fps (2 shutter WDR)	SXGA / HD 720P / XGA / SVGA / D1 / VGA / CIF / QCIF @50/60fps (2 shutter WDR) or 25/30fps (4 shutter WDR)
Protocol		IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF, ARP	
Security		HTTPS / IP Filter / IEEE 802.1X	
Event Notification		HTTP / FTP / SMTP	
Micro SD*		microSDHC 32GB support	
Supported Web Browser		Internet Explorer (6.0+) / Chrome / Firefox / Safari	
User Account		20	
Password Levels		User and Administrator	

Mechanical		
Lens Mounting		M12 Board Lens
Connectors	Ethernet	RJ-45

General	
Operating Temperature	-10°C ~ 50°C (14° ~ 122° F)
Humidity	10% ~ 90%, No Condensation
Weatherproof Standard	Rugged Type- IP66
Dimension	ø 110.2 x 47.7 mm (ø 4.3 x 1.9 in.)
Weight	180 g (0.40 lb)
Power Source	PoE
Power Consumption	4.2W
Regulatory	CE / FCC / RoHS

* mark for optional items
Product specification and availability are subject to change without notice.

DYNACOLOR always watching

DYNACOLOR, INC.
No. 116, Jou Tz Street, Neihu, Taipei 114, Taiwan
TEL: (886)2-2659-8898 FAX: (886)2-2659-8868
http://www.dynacolor.com.tw info@dynacolor.com.tw

SR16 SNVR

STANDALONE
NETWORK
VIDEO
RECORDER

ENREGISTREUR NUMERIQUE - 16 VOIES

SR16 Système MVR constitue le meilleur choix pour des applications de « surveillance » de petites et moyennes tailles telles que : les immeubles, les bureaux et les maisons. Il a une capacité 4 HDD et 16 voies "Mégapixels" de connexions Il permet un enregistrement stable et fiable - Il permettra également d'étendre vos projets avec notamment le logiciel libre Etro Centre CMS.

- Enregistrement caméras "Full" : 16 CH 30 FSP @ HD-1080p
- 4 r SATA HDD simplicité d'installation ME Conception
- Soutient pleinement toutes les options des caméras IP Etrovision
- Prise en charge gestion "multitechnique" NVR par EtroCenter CMS
- Prise en charge Etro Mobile : Mobile-client
- Prise en charge sur écrans

Distribué par :
CNM International – 94 avenue de la Sarriette – 13600 La Ciotat
Tel : 04 42 83 84 85 – Fax : 04 42 83 84 86 – contact-cnmi@wanadoo.fr

GUIDE D'HYGIÈNE INFORMATIQUE

RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES

AVANT-PROPOS

Paru en janvier 2013 dans sa première version, le Guide d'hygiène informatique édité par l'ANSSI s'adresse aux entités publiques ou privées dotées d'une direction des systèmes d'information (DSI) ou de professionnels dont la mission est de veiller à leur sécurité. Il est né du constat que si les mesures qui y sont édictées avaient été appliquées par les entités concernées, la majeure partie des attaques informatiques ayant requis une intervention de l'agence aurait pu être évitée.

Cette nouvelle version a fait l'objet d'une mise à jour portant à la fois sur les technologies et pratiques – nouvelles ou croissantes – avec lesquelles il s'agit de composer en matière de sécurité (nomadisme, séparation des usages, etc.) mais aussi sur la mise à disposition d'outils (indicateurs de niveau standard ou renforcé) pour éclairer le lecteur dans l'appréciation des mesures énoncées. Si l'objet de ce guide n'est pas la sécurité de l'information en tant que telle, appliquer les mesures proposées maximise la sécurité du système d'information, berceau des données de votre entité.

La sécurité n'est plus une option. À ce titre, les enjeux de sécurité numérique doivent se rapprocher des préoccupations économiques, stratégiques ou encore d'image qui sont celles des décideurs. En contextualisant le besoin, en rappelant l'objectif poursuivi et en y répondant par la mesure concrète correspondante, ce guide d'hygiène informatique est une feuille de route qui épouse les intérêts de toute entité consciente de la valeur de ses données.

SOMMAIRE

Le présent document comporte 42 règles de sécurité simples. Chacune d'entre elles est importante et vous pouvez tout à fait les considérer indépendamment les unes des autres pour améliorer votre niveau de sécurité sur quelques points particuliers.

Cependant, nous vous conseillons d'utiliser ce guide comme base pour définir un plan d'actions :

1. Commencez par établir un état des lieux pour chacune des règles grâce à l'outil de suivi qui se trouve en annexe de ce document. Pour chaque règle, déterminez si votre organisme atteint le niveau standard et, le cas échéant, le niveau renforcé.
2. Si vous ne pouvez pas faire cet état des lieux par manque de connaissance de votre système d'information, n'hésitez pas à solliciter l'aide d'un spécialiste pour procéder à un diagnostic et assurer un niveau de sécurité élémentaire. (À lire : ANSSI-CGPME, *Guide des bonnes pratiques de l'informatique*, mars 2015).
3. À partir du constat établi à cette première étape, visez en priorité les règles pour lesquelles vous n'avez pas encore atteint le niveau « standard », pour définir un premier plan d'actions. Si les mesures de ce guide doivent être appliquées dans le cadre d'un référentiel publié par l'ANSSI et sauf mention explicite, il s'agit des mesures de niveau « standard ».
4. Lorsque vous avez atteint partout le niveau « standard », vous pouvez définir un nouveau plan d'actions en visant le niveau « renforcé » pour les règles concernées.

I

SENSIBILISER ET FORMER

1 Former les équipes opérationnelles à la sécurité des systèmes d'information

/ STANDARD

Les équipes opérationnelles (administrateurs réseau, sécurité et système, chefs de projet, développeurs, RSSI) ont des accès privilégiés au système d'information. Elles peuvent, par inadvertance ou par méconnaissance des conséquences de certaines pratiques, réaliser des opérations génératrices de vulnérabilités.

Citons par exemple l'affectation de comptes disposant de trop nombreux privilèges par rapport à la tâche à réaliser, l'utilisation de comptes personnels pour exécuter des services ou tâches périodiques, ou encore le choix de mots de passe peu robustes donnant accès à des comptes privilégiés.

Les équipes opérationnelles, pour être à l'état de l'art de la sécurité des systèmes d'information, doivent donc suivre - à leur prise de poste puis à intervalles réguliers - des formations sur :

- la législation en vigueur ;
- les principaux risques et menaces ;
- le maintien en condition de sécurité ;
- l'authentification et le contrôle d'accès ;
- le paramétrage fin et le durcissement des systèmes ;
- le cloisonnement réseau ;
- et la journalisation.

Cette liste doit être précisée selon le métier des collaborateurs en considérant des aspects tels que l'intégration de la sécurité pour les chefs de projet, le développement sécurisé pour les développeurs, les référentiels de sécurité pour les RSSI, etc.
Il est par ailleurs nécessaire de faire mention de clauses spécifiques dans les contrats de prestation pour garantir une formation régulière à la sécurité des systèmes d'information du personnel externe et notamment les infogérants.

2 Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

/ STANDARD

Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. À ce titre et dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information à travers des actions de sensibilisation et de formation.

Ces dernières doivent être régulières, adaptées aux utilisateurs ciblés, peuvent prendre différentes formes (mails, affichage, réunions, espace intranet dédié, etc.) et aborder au minimum les sujets suivants :

- les objectifs et enjeux que rencontre l'entité en matière de sécurité des systèmes d'information ;
- les informations considérées comme sensibles ;
- les réglementations et obligations légales ;
- les règles et consignes de sécurité régissant l'activité quotidienne : respect de la politique de sécurité, non-connexion d'équipements personnels au réseau de l'entité, non-divulgation de mots de passe à un tiers, non-réutilisation de mots de passe professionnels dans la sphère privée et inversement, signalement d'événements suspects, etc. ;
- les moyens disponibles et participant à la sécurité du système : verrouillage systématique de la session lorsque l'utilisateur quitte son poste, outil de protection des mots de passe, etc.

/ RENFORCÉ

Pour renforcer ces mesures, l'élaboration et la signature d'une charte des moyens informatiques précisant les règles et consignes que doivent respecter les utilisateurs peut être envisagée.

ANSSI, *Charte d'utilisation des moyens informatiques et des outils numériques – Guide d'élaboration en 8 points clés pour les PME et ETI*, guide, juin 2017

3 Maîtriser les risques de l'infogérance

/ STANDARD

Lorsqu'une entité souhaite externaliser son système d'information ou ses données, elle doit en amont évaluer les risques spécifiques à l'infogérance (maîtrise du système d'information, actions à distance, hébergement mutualisé, etc.) afin de prendre en compte, dès la rédaction des exigences applicables au futur prestataire, les besoins et mesures de sécurité adaptés.
Les risques SSI inhérents à ce type de démarche peuvent être liés au contexte de l'opération d'externalisation mais aussi à des spécifications contractuelles déficientes ou incomplètes.

En faveur du bon déroulement des opérations, il s'agit donc :
> d'étudier attentivement les conditions des offres, la possibilité de les adapter à des besoins spécifiques et les limites de responsabilité du prestataire ;
> d'imposer une liste d'exigences précises au prestataire : réversibilité du contrat, réalisation d'audits, sauvegarde et restitution des données dans un format ouvert normalisé, maintien à niveau de la sécurité dans le temps, etc.

Pour formaliser ces engagements, le prestataire fournira au commanditaire un plan d'assurance sécurité (PAS) prévu par l'appel d'offre. Il s'agit d'un document contractuel décrivant l'ensemble des dispositions spécifiques que les candidats s'engagent à mettre en œuvre pour garantir le respect des exigences de sécurité spécifiées par l'entité.

Le recours à des solutions ou outils non maîtrisés (par exemple hébergés dans le nuage) n'est pas ici considéré comme étant du ressort de l'infogérance et par ailleurs déconseillé en cas de traitement d'informations sensibles.

ANSSI, *Guide de l'externalisation – Maîtriser les risques de l'infogérance*, guide, décembre 2010

II

CONNAÎTRE LE SYSTÈME D'INFORMATION

4 Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau

/STANDARD

Chaque entité possède des données sensibles. Ces dernières peuvent porter sur son activité propre (propriété intellectuelle, savoir-faire, etc.) ou sur ses clients, administrés ou usagers (données personnelles, contrats, etc.). Afin de pouvoir les protéger efficacement, il est indispensable de les identifier.

À partir de cette liste de données sensibles, il sera possible de déterminer sur quels composants du système d'information elles se localisent (bases de données, partages de fichiers, postes de travail, etc.). Ces composants correspondent aux serveurs et postes critiques pour l'entité. À ce titre, ils devront faire l'objet de mesures de sécurité spécifiques pouvant porter sur la sauvegarde, la journalisation, les accès, etc.

Il s'agit donc de créer et de maintenir à jour un schéma simplifié du réseau (ou cartographie) représentant les différentes zones IP et le plan d'adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs, etc.) et les interconnexions avec l'extérieur (Internet, réseaux privés, etc.) et les partenaires. Ce schéma doit également permettre de localiser les serveurs détenteurs d'informations sensibles de l'entité.

5 Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour

/STANDARD

Les comptes bénéficiant de droits spécifiques sont des cibles privilégiées par les attaquants qui souhaitent obtenir un accès le plus large possible au système d'information. Ils doivent donc faire l'objet d'une attention toute particulière. Il s'agit pour cela d'effectuer un inventaire de ces comptes, de le mettre à jour régulièrement et d'y renseigner les informations suivantes :

- les utilisateurs ayant un compte administrateur ou des droits supérieurs à ceux d'un utilisateur standard sur le système d'information ;
- les utilisateurs disposant de suffisamment de droits pour accéder aux répertoires de travail des responsables ou de l'ensemble des utilisateurs ;
- les utilisateurs utilisant un poste non administré par le service informatique et qui ne fait pas l'objet de mesures de sécurité édictées par la politique de sécurité générale de l'entité.

Il est fortement recommandé de procéder à une revue périodique de ces comptes afin de s'assurer que les accès aux éléments sensibles (notamment les répertoires de travail et la messagerie électronique des responsables) soient maitrisés. Ces revues permettront également de supprimer les accès devenus obsolètes suite au départ d'un utilisateur par exemple.

Enfin, il est souhaitable de définir et d'utiliser une nomenclature simple et claire pour identifier les comptes de services et les comptes d'administration. Cela facilitera notamment leur revue et la détection d'intrusion.

6 Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs

/STANDARD

Les effectifs d'une entité, qu'elle soit publique ou privée, évoluent sans cesse : arrivées, départs, mobilité interne. Il est par conséquent nécessaire que les droits et les accès au système d'information soient mis à jour en fonction de ces évolutions. Il est notamment essentiel que l'ensemble des droits affectés à une personne soient révoqués lors de son départ ou en cas de changement de fonction. Les procédures d'arrivée et de départ doivent donc être définies, en lien avec la fonction ressources humaines. Elles doivent au minimum prendre en compte :

- la création et la suppression des comptes informatiques et boîtes aux lettres associées ;
- les droits et accès à attribuer et retirer à une personne dont la fonction change ;
- la gestion des accès physiques aux locaux (attribution, restitution des badges et des clés, etc.) ;
- l'affectation des équipements mobiles (ordinateur portable, clé USB, disque dur, ordiphone, etc.) ;
- la gestion des documents et informations sensibles (transfert de mots de passe, changement des mots de passe ou des codes sur les systèmes existants).

/RENFORCÉ

Les procédures doivent être formalisées et mises à jour en fonction du contexte.

7 Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés

/STANDARD

Pour garantir la sécurité de son système d'information, l'entité doit maîtriser les équipements qui s'y connectent, chacun constituant un point d'entrée potentiellement vulnérable. Les équipements personnels (ordinateurs portables, tablettes, ordiphones, etc.) sont, par définition, difficilement maîtrisables dans la mesure où ce sont les utilisateurs qui décident de leur niveau de sécurité. De la même manière, la sécurité des équipements dont sont dotés les visiteurs échappe à tout contrôle de l'entité.

Seule la connexion de terminaux maîtrisés par l'entité doit être autorisée sur ses différents réseaux d'accès, qu'ils soient filaire ou sans fil. Cette recommandation, avant tout d'ordre organisationnel, est souvent perçue comme inacceptable ou rétrograde. Cependant, y déroger fragilise le réseau de l'entité et sert ainsi les intérêts d'un potentiel attaquant.

La sensibilisation des utilisateurs doit donc s'accompagner de solutions pragmatiques répondant à leurs besoins. Citons par exemple la mise à disposition d'un réseau Wi-Fi avec SSID dédié pour les terminaux personnels ou visiteurs.

/RENFORCÉ

Ces aménagements peuvent être complétés par des mesures techniques telles que l'authentification des postes sur le réseau (par exemple à l'aide du standard 802.1X ou d'un équivalent).

III

AUTHENTIFIER ET CONTRÔLER LES ACCÈS

8 Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur

/STANDARD

Afin de faciliter l'attribution d'une action sur le système d'information en cas d'incident ou d'identifier d'éventuels comptes compromis, les comptes d'accès doivent être nominatifs.

L'utilisation de comptes génériques (ex : *admin*, *user*) doit être marginale et ceux-ci doivent pouvoir être rattachés à un nombre limité de personnes physiques.

Bien entendu, cette règle n'interdit pas le maintien de comptes de service, rattachés à un processus informatique (ex : *apache*, *mysqld*).

Dans tous les cas, les comptes génériques et de service doivent être gérés selon une politique au moins aussi stricte que celle des comptes nominatifs. Par ailleurs, un compte d'administration nominatif, distinct du compte utilisateur, doit être attribué à chaque administrateur. Les identifiants et secrets d'authentification doivent être différents (ex : *pmartin* comme identifiant utilisateur, *adm-pmartin* comme identifiant administrateur). Ce compte d'administration, disposant de plus de privilèges, doit être dédié exclusivement aux actions d'administration. De plus, il doit être utilisé sur des environnements dédiés à l'administration afin de ne pas laisser de traces de connexion ni de condensat de mot de passe sur un environnement plus exposé.

/RENFORCÉ

Dès que possible la journalisation liée aux comptes (ex : relevé des connexions réussies/échouées) doit être activée.

9 Attribuer les bons droits sur les ressources sensibles du système d'information

/STANDARD

Certaines des ressources du système peuvent constituer une source d'information précieuse aux yeux d'un attaquant (répertoires contenant des données sensibles, bases de données, boîtes aux lettres électroniques, etc.). Il est donc primordial d'établir une liste précise de ces ressources et pour chacune d'entre elles :

- de définir quelle population peut y avoir accès ;
- de contrôler strictement son accès, en s'assurant que les utilisateurs sont authentifiés et font partie de la population ciblée ;
- d'éviter sa dispersion et sa duplication à des endroits non maîtrisés ou soumis à un contrôle d'accès moins strict.

Par exemple, les répertoires des administrateurs regroupant de nombreuses informations sensibles doivent faire l'objet d'un contrôle d'accès précis. Il en va de même pour les informations sensibles présentes sur des partages réseau : exports de fichiers de configuration, documentation technique du système d'information, bases de données métier, etc. Une revue régulière des droits d'accès doit par ailleurs être réalisée afin d'identifier les accès non autorisés.

10 Définir et vérifier des règles de choix et de dimensionnement des mots de passe

/STANDARD

L'ANSSI énonce un ensemble de règles et de bonnes pratiques en matière de choix et de dimensionnement des mots de passe. Parmi les plus critiques de ces règles figure la sensibilisation des utilisateurs aux risques liés au choix d'un mot de passe qui serait trop facile à deviner, ou encore la réutilisation de mots de passe d'une application à l'autre et plus particulièrement entre messageries personnelles et professionnelles.

Pour encadrer et vérifier l'application de ces règles de choix et de dimensionnement, l'entité pourra recourir à différentes mesures parmi lesquelles :

> le blocage des comptes à l'issue de plusieurs échecs de connexion ;
> la désactivation des options de connexion anonyme ;
> l'utilisation d'un outil d'audit de la robustesse des mots de passe.

En amont de telles procédures, un effort de communication visant à expliquer le sens de ces règles et éveiller les consciences sur leur importance est fondamental.

ANSSI, *Recommandations de sécurité relatives aux mots de passe*, note technique, juin 2012

11 Protéger les mots de passe stockés sur les systèmes

/STANDARD

La complexité, la diversité ou encore l'utilisation peu fréquente de certains mots de passe, peuvent encourager leur stockage sur un support physique (mémo, post-it) ou numérique (fichiers de mots de passe, envoi par mail à soi-même, recours aux boutons « Se souvenir du mot de passe ») afin de pallier tout oubli ou perte.

Or, les mots de passe sont une cible privilégiée par les attaquants désireux d'accéder au système, que cela fasse suite à un vol ou à un éventuel partage du support de stockage. C'est pourquoi ils doivent impérativement être protégés au moyen de solutions sécurisées au premier rang desquelles figurent l'utilisation d'un coffre-fort numérique et le recours à des mécanismes de chiffrement.

Bien entendu, le choix d'un mot de passe pour ce coffre-fort numérique doit respecter les règles énoncées précédemment et être mémorisé par l'utilisateur, qui n'a plus que celui-ci à retenir.

12 Changer les éléments d'authentification par défaut sur les équipements et services

/STANDARD

Il est impératif de partir du principe que les configurations par défaut des systèmes d'information sont systématiquement connues des attaquants, quand bien même celles-ci ne le sont pas du grand public. Ces configurations se révèlent (trop) souvent triviales (mot de passe identique à l'identifiant, mal dimensionné ou commun à l'ensemble des équipements et services par exemple) et sont, la plupart du temps, faciles à obtenir pour des attaquants capables de se faire passer pour un utilisateur légitime.

Les éléments d'authentification par défaut des composants du système doivent donc être modifiés dès leur installation et, s'agissant de mots de passe, être conformes aux recommandations précédentes en matière de choix, de dimensionnement et de stockage.

Si le changement d'un identifiant par défaut se révèle impossible pour cause, par exemple, de mot de passe ou certificat « en dur » dans un équipement, ce problème critique doit être signalé au distributeur du produit afin que cette vulnérabilité soit corrigée au plus vite.

/RENFORCÉ

Afin de limiter les conséquences d'une compromission, il est par ailleurs essentiel, après changement des éléments d'authentification par défaut, de procéder à leur renouvellement régulier.

13 Privilégier lorsque c'est possible une authentification forte

/STANDARD

Il est vivement recommandé de mettre en œuvre une authentification forte nécessitant l'utilisation de deux facteurs d'authentification différents parmi les suivants :

> quelque chose que je sais (mot de passe, tracé de déverrouillage, signature) ;
> quelque chose que je possède (carte à puce, jeton USB, carte magnétique, RFID, un téléphone pour recevoir un code SMS) ;
> quelque chose que je suis (une empreinte biométrique).

/RENFORCÉ

Les cartes à puces doivent être privilégiées ou, à défaut, les mécanismes de mots de passe à usage unique (ou *One Time Password*) avec jeton physique. Les opérations cryptographiques mises en place dans ces deux facteurs offrent généralement de bonnes garanties de sécurité.

Les cartes à puce peuvent être plus complexes à mettre en place car nécessitant une infrastructure de gestion des clés adaptée. Elles présentent cependant l'avantage d'être réutilisables à plusieurs fins : chiffrement, authentification de messagerie, authentification sur le poste de travail, etc.

IV

SÉCURISER LES POSTES

14 Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique

/STANDARD

L'utilisateur plus ou moins au fait des bonnes pratiques de sécurité informatique est, dans de très nombreux cas, la première porte d'entrée des attaquants vers le système. Il est donc fondamental de mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique de l'entité (postes utilisateurs, serveurs, imprimantes, téléphones, périphériques USB, etc.) en implémentant les mesures suivantes :

- limiter les applications installées et modules optionnels des navigateurs web aux seuls nécessaires ;
- doter les postes utilisateurs d'un pare-feu local et d'un anti-virus (ceux-ci sont parfois inclus dans le système d'exploitation) ;
- chiffrer les partitions où sont stockées les données des utilisateurs ;
- désactiver les exécutions automatiques (autorun).

En cas de dérogation nécessaire aux règles de sécurité globales applicables aux postes, ceux-ci doivent être isolés du système (s'il est impossible de mettre à jour certaines applications pour des raisons de compatibilité par exemple).

/RENFORCÉ

Les données vitales au bon fonctionnement de l'entité que détiennent les postes utilisateurs et les serveurs doivent faire l'objet de sauvegardes régulières et stockées sur des équipements déconnectés, et leur restauration doit être vérifiée de manière périodique. En effet, de plus en plus de petites structures font l'objet d'attaques rendant ces données indisponibles (par exemple pour exiger en contrepartie de leur restitution le versement d'une somme conséquente (rançongiciel)).

15 Se protéger des menaces relatives à l'utilisation de supports amovibles

/STANDARD

Les supports amovibles peuvent être utilisés afin de propager des virus, voler des informations sensibles et stratégiques ou encore compromettre le réseau de l'entité. De tels agissements peuvent avoir des conséquences désastreuses pour l'activité de la structure ciblée.

S'il n'est pas question d'interdire totalement l'usage de supports amovibles au sein de l'entité, il est néanmoins nécessaire de traiter ces risques en identifiant des mesures adéquates et en sensibilisant les utilisateurs aux risques que ces supports peuvent véhiculer.

Il convient notamment de proscrire le branchement de clés USB inconnues (ramassées dans un lieu public par exemple) et de limiter au maximum celui de clés non maîtrisées (dont on connait la provenance mais pas l'intégrité) sur le système d'information à moins, dans ce dernier cas, de faire inspecter leur contenu par l'antivirus du poste de travail.

/RENFORCÉ

Sur les postes utilisateur, il est recommandé d'utiliser des solutions permettant d'interdire l'exécution de programmes sur les périphériques amovibles (par exemple Applocker sous Windows ou des options de montage *noexec* sous Unix).

Lors de la fin de vie des supports amovibles, il sera nécessaire d'implémenter et de respecter une procédure de mise au rebut stricte pouvant aller jusqu'à leur destruction sécurisée afin de limiter la fuite d'informations sensibles.

ANSSI, *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*, note technique, décembre 2013

ANSSI, *Recommandations de configuration d'un système GNU/Linux*, note technique, janvier 2016

16 Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité

/STANDARD

La sécurité du système d'information repose sur la sécurité du maillon le plus faible. Il est donc nécessaire d'homogénéiser la gestion des politiques de sécurité s'appliquant à l'ensemble du parc informatique de l'entité.

L'application de ces politiques (gestion des mots de passe, restrictions de connexions sur certains postes sensibles, configuration des navigateurs Web, etc.) doit être simple et rapide pour les administrateurs, en vue notamment de faciliter la mise en œuvre de contre-mesures en cas de crise informatique.

Pour cela, l'entité pourra se doter d'un outil de gestion centralisée (par exemple Active Directory en environnement Microsoft) auquel il s'agit d'inclure le plus grand nombre d'équipements informatiques possible. Les postes de travail et les serveurs sont concernés par cette mesure qui nécessite éventuellement en amont un travail d'harmonisation des choix de matériels et de systèmes d'exploitation.

Ainsi, des politiques de durcissement du système d'exploitation ou d'applications pourront facilement s'appliquer depuis un point central tout en favorisant la réactivité attendue en cas de besoin de reconfiguration.

ANSSI, *Recommandations de sécurité relatives à Active Directory*, note technique, septembre 2014

17 Activer et configurer le pare-feu local des postes de travail

/STANDARD

Après avoir réussi à prendre le contrôle d'un poste de travail (à cause, par exemple, d'une vulnérabilité présente dans le navigateur Internet), un attaquant cherchera souvent à étendre son intrusion aux autres postes de travail pour, *in fine*, accéder aux documents des utilisateurs.

Afin de rendre plus difficile ce déplacement latéral de l'attaquant, il est nécessaire d'activer le pare-feu local des postes de travail au moyen de logiciels intégrés (pare-feu local Windows) ou spécialisés.

Les flux de poste à poste sont en effet très rares dans un réseau bureautique classique : les fichiers sont stockés dans des serveurs de fichiers, les applications accessibles sur des serveurs métier, etc.

/RENFORCÉ

Le filtrage le plus simple consiste à bloquer l'accès aux ports d'administration par défaut des postes de travail (ports TCP 135, 445 et 3389 sous Windows, port TCP 22 sous Unix), excepté depuis les ressources explicitement identifiées (postes d'administration et d'assistance utilisateur, éventuels serveurs de gestion requérant l'accès à des partages réseau sur les postes, etc.).

Une analyse des flux entrants utiles (administration, logiciels d'infrastructure, applications particulières, etc.) doit être menée pour définir la liste des autorisations à configurer. Il est préférable de bloquer l'ensemble des flux par défaut et de n'autoriser que les services nécessaires depuis les équipements correspondants (« liste blanche »).

Le pare-feu doit également être configuré pour journaliser les flux bloqués, et ainsi identifier les erreurs de configuration d'applications ou les tentatives d'intrusion.

18 Chiffrer les données sensibles transmises par voie Internet

/STANDARD

Internet est un réseau sur lequel il est quasi impossible d'obtenir des garanties sur le trajet que vont emprunter les données que l'on y envoie. Il est donc tout à fait possible qu'un attaquant se trouve sur le trajet de données transitant entre deux correspondants.

Toutes les données envoyées par courriel ou transmises au moyen d'outils d'hébergement en ligne (Cloud) sont par conséquent vulnérables. Il s'agit donc de procéder à leur chiffrement systématique avant de les adresser à un correspondant ou de les héberger.

La transmission du secret (mot de passe, clé, etc.) permettant alors de déchiffrer les données, si elle est nécessaire, doit être effectuée via un canal de confiance ou, à défaut, un canal distinct du canal de transmission des données. Ainsi, si les données chiffrées sont transmises par courriel, une remise en main propre du mot de passe ou, à défaut, par téléphone doit être privilégiée.

Catalogue des produits et prestataires de service qualifiés

V

SÉCURISER LE RÉSEAU

19 Segmenter le réseau et mettre en place un cloisonnement entre ces zones

/STANDARD

Lorsque le réseau est « à plat », sans aucun mécanisme de cloisonnement, chaque machine du réseau peut accéder à n'importe quelle autre machine. La compromission de l'une d'elles met alors en péril l'ensemble des machines connectées. Un attaquant peut ainsi compromettre un poste utilisateur et ensuite « rebondir » jusqu'à des serveurs critiques.

Il est donc important, dès la conception de l'architecture réseau, de raisonner par segmentation en zones composées de systèmes ayant des besoins de sécurité homogènes. On pourra par exemple regrouper distinctement des serveurs d'infrastructure, des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, etc.

Une zone se caractérise alors par des VLAN et des sous-réseaux IP dédiés voire par des infrastructures dédiées selon sa criticité. Ainsi, des mesures de cloisonnement telles qu'un filtrage IP à l'aide d'un pare-feu peuvent être mises en place entre les différentes zones. On veillera en particulier à cloisonner autant que possible les équipements et flux associés aux tâches d'administration.

Pour les réseaux dont le cloisonnement a posteriori ne serait pas aisé, il est recommandé d'intégrer cette démarche dans toute nouvelle extension du réseau ou à l'occasion d'un renouvellement d'équipements.

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013

20 S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages

/STANDARD

L'usage du Wi-Fi en milieu professionnel est aujourd'hui démocratisé mais présente toujours des risques de sécurité bien spécifiques : faibles garanties en matière de disponibilité, pas de maîtrise de la zone de couverture pouvant mener à une attaque hors du périmètre géographique de l'entité, configuration par défaut des points d'accès peu sécurisée, etc.

La segmentation de l'architecture réseau doit permettre de limiter les conséquences d'une intrusion par voie radio à un périmètre déterminé du système d'information. Les flux en provenance des postes connectés au réseau d'accès Wi-Fi doivent donc être filtrés et restreints aux seuls flux nécessaires.

De plus, il est important d'avoir recours prioritairement à un chiffrement robuste (mode WPA2, algorithme AES CCMP) et à une authentification centralisée, si possible par certificats clients des machines.

La protection du réseau Wi-Fi par un mot de passe unique et partagé est déconseillée. À défaut, il doit être complexe et son renouvellement prévu mais il ne doit en aucun cas être diffusé à des tiers non autorisés.

Les points d'accès doivent par ailleurs être administrés de manière sécurisée (ex : interface dédiée, modification du mot de passe administrateur par défaut).

Enfin, toute connexion Wi-Fi de terminaux personnels ou visiteurs (ordinateurs portables, ordiphones) doit être séparée des connexions Wi-Fi des terminaux de l'entité (ex : SSID et VLAN distincts, accès Internet dédié).

ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi*, note technique, septembre 2013

21 Utiliser des protocoles réseaux sécurisés dès qu'ils existent

/STANDARD

Si aujourd'hui la sécurité n'est plus optionnelle, cela n'a pas toujours été le cas. C'est pourquoi de nombreux protocoles réseaux ont dû évoluer pour intégrer cette composante et répondre aux besoins de confidentialité et d'intégrité qu'impose l'échange de données. Les protocoles réseaux sécurisés doivent être utilisés dès que possible, que ce soit sur des réseaux publics (Internet par exemple) ou sur le réseau interne de l'entité.

Bien qu'il soit difficile d'en dresser une liste exhaustive, les protocoles les plus courants reposent sur l'utilisation de TLS et sont souvent identifiables par l'ajout de la lettre « s » (pour *secure* en anglais) à l'acronyme du protocole. Citons par exemple HTTPS pour la navigation Web ou IMAPS, SMTPS ou POP3S pour la messagerie.

D'autres protocoles ont été conçus de manière sécurisée dès la conception pour se substituer à d'anciens protocoles non sécurisés. Citons par exemple SSH (*Secure SHell*) venu remplacer les protocoles de communication historiques TELNET et RLOGIN.

ANSSI, *Recommandations pour un usage sécurisé d'[OPEN] SSH*, note technique, août 2016

22 Mettre en place une passerelle d'accès sécurisé à Internet

/STANDARD

L'accès à Internet, devenu indispensable, présente des risques importants : sites Web hébergeant du code malveillant, téléchargement de fichiers « toxiques » et, par conséquent, possible prise de contrôle du terminal, fuite de données sensibles, etc. Pour sécuriser cet usage, il est donc indispensable que les terminaux utilisateurs n'aient pas d'accès réseau direct à Internet.

C'est pourquoi il est recommandé de mettre en œuvre une passerelle sécurisée d'accès à Internet comprenant au minimum un pare-feu au plus près de l'accès Internet pour filtrer les connexions et un serveur mandataire (proxy) embarquant différents mécanismes de sécurité. Celui-ci assure notamment l'authentification des utilisateurs et la journalisation des requêtes.

/RENFORCÉ

Des mécanismes complémentaires sur le serveur mandataire pourront être activés selon les besoins de l'entité : analyse antivirus du contenu, filtrage par catégories d'URLs, etc. Le maintien en condition de sécurité des équipements de la passerelle est essentiel, il fera donc l'objet de procédures à respecter. Suivant le nombre de collaborateurs et le besoin de disponibilité, ces équipements pourront être redondés.

Par ailleurs, pour les terminaux utilisateurs, les résolutions DNS en direct de noms de domaines publics seront par défaut désactivées, celles-ci étant déléguées au serveur mandataire.

Enfin, il est fortement recommandé que les postes nomades établissent au préalable une connexion sécurisée au système d'information de l'entité pour naviguer de manière sécurisée sur le Web à travers la passerelle.

23 Cloisonner les services visibles depuis Internet du reste du système d'information

/STANDARD

Une entité peut choisir d'héberger en interne des services visibles sur Internet (site web, serveur de messagerie, etc.). Au regard de l'évolution et du perfectionnement des cyberattaques sur Internet, il est essentiel de garantir un haut niveau de protection de ce service avec des administrateurs compétents, formés de manière continue (à l'état de l'art des technologies en la matière) et disponibles. Dans le cas contraire, le recours à un hébergement externalisé auprès de professionnels est à privilégier.

De plus, les infrastructures d'hébergement Internet doivent être physiquement cloisonnées de toutes les infrastructures du système d'information qui n'ont pas vocation à être visibles depuis Internet.

Enfin, il convient de mettre en place une infrastructure d'interconnexion de ces services avec Internet permettant de filtrer les flux liés à ces services de manière distincte des autres flux de l'entité. Il s'agit également d'imposer le passage des flux entrants par un serveur mandataire inverse (*reverse proxy*) embarquant différents mécanismes de sécurité.

ANSSI, *Guide de définition d'une architecture de passerelle d'interconnexion sécurisée*, note technique, décembre 2011

ANSSI, *Maîtriser les risques de l'infogérance*, guide, décembre 2010

24 Protéger sa messagerie professionnelle

/STANDARD

La messagerie est le principal vecteur d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant.

Les utilisateurs doivent être particulièrement sensibilisés à ce sujet : l'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) est nécessaire.

Pour se prémunir d'escroqueries (ex : demande de virement frauduleux émanant vraisemblablement d'un dirigeant), des mesures organisationnelles doivent être appliquées strictement.

Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue une fuite irrémédiable d'informations de l'entité. Si nécessaire des moyens maîtrisés et sécurisés pour l'accès distant à la messagerie professionnelle doivent être proposés.

Que l'entité héberge ou fasse héberger son système de messagerie, elle doit s'assurer :

> de disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs pour prévenir la réception de fichiers infectés ;
> de l'activation du chiffrement TLS des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateur et les serveurs hébergeant les boîtes aux lettres.

/RENFORCÉ

Il est souhaitable de ne pas exposer directement les serveurs de boîte aux lettres sur Internet. Dans ce cas, un serveur relai dédié à l'envoi et à la réception des messages doit être mis en place en coupure d'Internet.

Alors que le spam - malveillant ou non - constitue la majorité des courriels échangés sur Internet, le déploiement d'un service anti-spam doit permettre d'éliminer cette source de risques.

Enfin, l'administrateur de messagerie s'assurera de la mise en place des mécanismes de vérification d'authenticité et de la bonne configuration des enregistrements DNS publics liés à son infrastructure de messagerie (MX, SPF, DKIM, DMARC).

ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*, guide, février 2015

25 Sécuriser les interconnexions réseau dédiées avec les partenaires

/STANDARD

Pour des besoins opérationnels, une entité peut être amenée à établir une interconnexion réseau dédiée avec un fournisseur ou un client (ex : infogérance, échange de données informatisées, flux monétiques, etc.).

Cette interconnexion peut se faire au travers d'un lien sur le réseau privé de l'entité ou directement sur Internet. Dans le second cas, il convient d'établir un tunnel site à site, de préférence IPsec, en respectant les préconisations de l'ANSSI.

Le partenaire étant considéré par défaut comme non sûr, il est indispensable d'effectuer un filtrage IP à l'aide d'un pare-feu au plus près de l'entrée des flux sur le réseau de l'entité. La matrice des flux (entrants et sortants) devra être réduite au juste besoin opérationnel, maintenue dans le temps et la configuration des équipements devra y être conforme.

/RENFORCÉ

Pour des entités ayant des besoins de sécurité plus exigeants, il conviendra de s'assurer que l'équipement de filtrage IP pour les connexions partenaires est dédié à cet usage. L'ajout d'un équipement de détection d'intrusions peut également constituer une bonne pratique.

Par ailleurs la connaissance d'un point de contact à jour chez le partenaire est nécessaire pour pouvoir réagir en cas d'incident de sécurité.

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, note technique, août 2015

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013

26 Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

/STANDARD

Les mécanismes de sécurité physique doivent faire partie intégrante de la sécurité des systèmes d'information et être à l'état de l'art afin de s'assurer qu'ils ne puissent pas être contournés aisément par un attaquant. Il convient donc d'identifier les mesures de sécurité physique adéquates et de sensibiliser continuellement les utilisateurs aux risques engendrés par le contournement des règles.

Les accès aux salles serveurs et aux locaux techniques doivent être contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge. Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont à proscrire, sauf s'il est possible de tracer strictement les accès et de limiter ces derniers en fonction des plages horaires. Une revue des droits d'accès doit être réalisée régulièrement afin d'identifier les accès non autorisés.

Lors du départ d'un collaborateur ou d'un changement de prestataire, il est nécessaire de procéder au retrait des droits d'accès ou au changement des codes d'accès.

Enfin, les prises réseau se trouvant dans des zones ouvertes au public (salle de réunion, hall d'accueil, couloirs, placards, etc.) doivent être restreintes ou désactivées afin d'empêcher un attaquant de gagner facilement l'accès au réseau de l'entreprise.

VI

SÉCURISER L'ADMINISTRATION

27 Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information

/STANDARD

Un poste de travail ou un serveur utilisé pour les actions d'administration ne doit en aucun cas avoir accès à Internet, en raison des risques que la navigation Web (à travers des sites contenant du code malveillant) et la messagerie (au travers de pièces jointes potentiellement vérolées) font peser sur son intégrité.

Pour les autres usages des administrateurs nécessitant Internet (consultation de documentation en ligne, de leur messagerie, etc.), il est recommandé de mettre à leur disposition un poste de travail distinct. À défaut, l'accès à une infrastructure virtualisée distante pour la bureautique depuis un poste d'administration est envisageable. La réciproque consistant à fournir un accès distant à une infrastructure d'administration depuis un poste bureautique est déconseillée car elle peut mener à une élévation de privilèges en cas de récupération des authentifiants d'administration.

/RENFORCÉ

Concernant les mises à jour logicielles des équipements administrés, elles doivent être récupérées depuis une source sûre (le site de l'éditeur par exemple), contrôlées puis transférées sur le poste ou le serveur utilisé pour l'administration et non connecté à Internet. Ce transfert peut être réalisé sur un support amovible dédié.

Pour des entités voulant automatiser certaines tâches, la mise en place d'une zone d'échanges est conseillée.

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, février 2015

28 Utiliser un réseau dédié et cloisonné pour l'administration du système d'information

/STANDARD

Un réseau d'administration interconnecte, entre autres, les postes ou serveurs d'administration et les interfaces d'administration des équipements. Dans la logique de segmentation du réseau global de l'entité, il est indispensable de cloisonner spécifiquement le réseau d'administration, notamment vis-à-vis du réseau bureautique des utilisateurs, pour se prémunir de toute compromission par rebond depuis un poste utilisateur vers une ressource d'administration.

Selon les besoins de sécurité de l'entité, il est recommandé :

- de privilégier en premier lieu un cloisonnement physique des réseaux dès que cela est possible, cette solution pouvant représenter des coûts et un temps de déploiement importants ; /RENFORCÉ
- à défaut, de mettre en œuvre un cloisonnement logique cryptographique reposant sur la mise en place de tunnels IPsec. Ceci permet d'assurer l'intégrité et la confidentialité des informations véhiculées sur le réseau d'administration vis-à-vis du réseau bureautique des utilisateurs ; /STANDARD
- au minimum, de mettre en œuvre un cloisonnement logique par VLAN. /STANDARD

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, février 2015

29 Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail

/STANDARD

De nombreux utilisateurs, y compris au sommet des hiérarchies, sont tentés de demander à leur service informatique de pouvoir disposer, par analogie avec leur usage personnel, de privilèges plus importants sur leurs postes de travail : installation de logiciels, configuration du système, etc. Par défaut, il est recommandé qu'un utilisateur du SI, quelle que soit sa position hiérarchique et ses attributions, ne dispose pas de privilèges d'administration sur son poste de travail. Cette mesure, apparemment contraignante, vise à limiter les conséquences de l'exécution malencontreuse d'un code malveillant. La mise à disposition d'un magasin étoffé d'applications validées par l'entité du point de vue de la sécurité permettra de répondre à la majorité des besoins.

Par conséquent, seuls les administrateurs chargés de l'administration des postes doivent disposer de ces droits lors de leurs interventions.

Si une délégation de privilèges sur un poste de travail est réellement nécessaire pour répondre à un besoin ponctuel de l'utilisateur, celle-ci doit être tracée, limitée dans le temps et retirée à échéance.

VII

GÉRER LE NOMADISME

30 Prendre des mesures de sécurisation physique des terminaux nomades

/STANDARD

Les terminaux nomades (ordinateurs portables, tablettes, ordiphones) sont, par nature, exposés à la perte et au vol. Ils peuvent contenir localement des informations sensibles pour l'entité et constituer un point d'entrée vers de plus amples ressources du système d'information. Au-delà de l'application au minimum des politiques de sécurité de l'entité, des mesures spécifiques de sécurisation de ces équipements sont donc à prévoir.

En tout premier lieu, les utilisateurs doivent être sensibilisés pour augmenter leur niveau de vigilance lors de leurs déplacements et conserver leurs équipements à portée de vue. N'importe quelle entité, même de petite taille, peut être victime d'une attaque informatique. Dès lors, en mobilité, tout équipement devient une cible potentielle voire privilégiée.

Il est recommandé que les terminaux nomades soient aussi banalisés que possible en évitant toute mention explicite de l'entité d'appartenance (par l'apposition d'un autocollant aux couleurs de l'entité par exemple).

Pour éviter toute indiscrétion lors de déplacements, notamment dans les transports ou les lieux d'attente, un filtre de confidentialité doit être positionné sur chaque écran.

/RENFORCÉ

Enfin, afin de rendre inutilisable le poste seul, l'utilisation d'un support externe complémentaire (carte à puce ou jeton USB par exemple) pour conserver des secrets de déchiffrement ou d'authentification peut être envisagée. Dans ce cas il doit être conservé à part.

ANSSI-CDSE, *Passeport de conseils aux voyageurs*, bonnes pratiques, janvier 2010

31 Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable

/STANDARD

Les déplacements fréquents en contexte professionnel et la miniaturisation du matériel informatique conduisent souvent à la perte ou au vol de celui-ci dans l'espace public. Cela peut porter atteinte aux données sensibles de l'entité qui y sont stockées.

Il faut donc ne stocker que des données préalablement chiffrées sur l'ensemble des matériels nomades (ordinateurs portables, ordiphones, clés USB, disques durs externes, etc.) afin de préserver leur confidentialité. Seul un secret (mot de passe, carte à puce, code PIN, etc.) pourra permettre à celui qui le possède d'accéder à ces données.

Une solution de chiffrement de partition, d'archives ou de fichier peut être envisagée selon les besoins. Là encore, il est essentiel de s'assurer de l'unicité et de la robustesse du secret de déchiffrement utilisé.

Dans la mesure du possible, il est conseillé de commencer par un chiffrement complet du disque avant d'envisager le chiffrement d'archives ou de fichiers. En effet, ces derniers répondent à des besoins différents et peuvent potentiellement laisser sur le support de stockage des informations non chiffrées (fichiers de restauration de suite bureautique, par exemple).

Catalogue des produits et prestataires de service qualifiés

32 Sécuriser la connexion réseau des postes utilisés en situation de nomadisme

/STANDARD

En situation de nomadisme, il n'est pas rare qu'un utilisateur ait besoin de se connecter au système d'information de l'entité. Il convient par conséquent de s'assurer du caractère sécurisé de cette connexion réseau à travers Internet. Même si la possibilité d'établir des tunnels VPN SSL/TLS est aujourd'hui courante, il est fortement recommandé d'établir un tunnel VPN IPsec entre le poste nomade et une passerelle VPN IPsec mise à disposition par l'entité.

Pour garantir un niveau de sécurité optimal, ce tunnel VPN IPsec doit être automatiquement établi et ne pas être débrayable par l'utilisateur, c'est-à-dire qu'aucun flux ne doit pouvoir être transmis en dehors de ce tunnel.

Pour les besoins spécifiques d'authentification aux portails captifs, l'entité peut choisir de déroger à la connexion automatique en autorisant une connexion à la demande ou maintenir cette recommandation en encourageant l'utilisateur à utiliser un partage de connexion sur un téléphone mobile de confiance.

/RENFORCÉ

Afin d'éviter toute réutilisation d'authentifiants depuis un poste volé ou perdu (identifiant et mot de passe enregistrés par exemple), il est préférable d'avoir recours à une authentification forte, par exemple avec un mot de passe et un certificat stocké sur un support externe (carte à puce ou jeton USB) ou un mécanisme de mot de passe à usage unique (*One Time Password*).

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, note technique, août 2015

33 Adopter des politiques de sécurité dédiées aux terminaux mobiles

/STANDARD

Les ordiphones et tablettes font partie de notre quotidien personnel et/ou professionnel. La première des recommandations consiste justement à ne pas mutualiser les usages personnel et professionnel sur un seul et même terminal, par exemple en ne synchronisant pas simultanément comptes professionnel et personnel de messagerie, de réseaux sociaux, d'agendas, etc.

Les terminaux, fournis par l'entité et utilisés en contexte professionnel doivent faire l'objet d'une sécurisation à part entière, dès lors qu'ils se connectent au système d'information de l'entité ou qu'ils contiennent des informations professionnelles potentiellement sensibles (mails, fichiers partagés, contacts, etc.). Dès lors, l'utilisation d'une solution de gestion centralisée des équipements mobiles est à privilégier. Il sera notamment souhaitable de configurer de manière homogène les politiques de sécurité inhérentes : moyen de déverrouillage du terminal, limitation de l'usage du magasin d'applications à des applications validées du point de vue de la sécurité, etc.

Dans le cas contraire, une configuration préalable avant remise de l'équipement et une séance de sensibilisation des utilisateurs est souhaitable.

/RENFORCÉ

Entre autres usages potentiellement risqués, celui d'un assistant vocal intégré augmente sensiblement la surface d'attaque du terminal et des cas d'attaque ont été démontrés. Pour ces raisons, il est donc déconseillé.

ANSSI, *Recommandations de sécurité relatives aux ordiphones*, note technique, juillet 2015

VIII

MAINTENIR LE SYSTÈME D'INFORMATION À JOUR

34 Définir une politique de mise à jour des composants du système d'information

/STANDARD

De nouvelles failles sont régulièrement découvertes au cœur des systèmes et logiciels. Ces dernières sont autant de portes d'accès qu'un attaquant peut exploiter pour réussir son intrusion dans le système d'information. Il est donc primordial de s'informer de l'apparition de nouvelles vulnérabilités (CERT-FR) et d'appliquer les correctifs de sécurité sur l'ensemble des composants du système dans le mois qui suit leur publication par l'éditeur. Une politique de mise à jour doit ainsi être définie et déclinée en procédures opérationnelles.

Celles-ci doivent notamment préciser :

- la manière dont l'inventaire des composants du système d'information est réalisé ;
- les sources d'information relatives à la publication des mises à jour ;
- les outils pour déployer les correctifs sur le parc (par exemple WSUS pour les mises à jour des composants Microsoft, des outils gratuits ou payants pour les composants tiers et autres systèmes d'exploitation) ;
- l'éventuelle qualification des correctifs et leur déploiement progressif sur le parc.

Les composants obsolètes qui ne sont plus supportés par leurs fabricants doivent être isolés du reste du système. Cette recommandation s'applique aussi bien au niveau réseau par un filtrage strict des flux, qu'au niveau des secrets d'authentification qui doivent être dédiés à ces systèmes.

CERT-FR : au sein du COSSI, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) assure le rôle de CERT (pour Computer Emergency Response Team) gouvernemental français. À ce titre, il compte parmi ses missions principales une action de veille technologique informant tout un chacun sur l'état de l'art des systèmes et logiciels.

35 Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles

/STANDARD

L'utilisation d'un système ou d'un logiciel obsolète augmente significativement les possibilités d'attaque informatique. Les systèmes deviennent vulnérables dès lors que les correctifs ne sont plus proposés. En effet, des outils malveillants exploitant ces vulnérabilités peuvent se diffuser rapidement sur Internet alors même que l'éditeur ne propose pas de correctif de sécurité.

Pour anticiper ces obsolescences, un certain nombre de précautions existent :

- établir et tenir à jour un inventaire des systèmes et applications du système d'information ;
- choisir des solutions dont le support est assuré pour une durée correspondant à leur utilisation ;
- assurer un suivi des mises à jour et des dates de fin de support des logiciels ;
- maintenir un parc logiciel homogène (la coexistence de versions différentes d'un même produit multiplie les risques et complique le suivi) ;
- limiter les adhérences logicielles, c'est-à-dire les dépendances de fonctionnement d'un logiciel par rapport à un autre, en particulier lorsque le support de ce dernier arrive à son terme ;
- inclure dans les contrats avec les prestataires et fournisseurs des clauses garantissant le suivi des correctifs de sécurité et la gestion des obsolescences ;
- identifier les délais et ressources nécessaires (matérielles, humaines, budgétaires) à la migration de chaque logiciel en fin de vie (tests de non-régression, procédure de sauvegarde, procédure de migration des données, etc.).

IX

SUPERVISER, AUDITER, RÉAGIR

36 Activer et configurer les journaux des composants les plus importants

/STANDARD

Disposer de journaux pertinents est nécessaire afin de pouvoir détecter d'éventuels dysfonctionnements et tentatives d'accès illicites aux composants du système d'information.

La première étape consiste à déterminer quels sont les composants critiques du système d'information. Il peut notamment s'agir des équipements réseau et de sécurité, des serveurs critiques, des postes de travail d'utilisateurs sensibles, etc.

Pour chacun, il convient d'analyser la configuration des éléments journalisés (format, fréquence de rotation des fichiers, taille maximale des fichiers journaux, catégories d'évènements enregistrés, etc.) et de l'adapter en conséquence. Les évènements critiques pour la sécurité doivent être journalisés et gardés pendant au moins un an (ou plus en fonction des obligations légales du secteur d'activités).

Une étude contextuelle du système d'information doit être effectuée et les éléments suivants doivent être journalisés :

- pare-feu : paquets bloqués ;
- systèmes et applications : authentifications et autorisations (échecs et succès), arrêts inopinés ;
- services : erreurs de protocoles (par exemples les erreurs 403, 404 et 500 pour les services HTTP), traçabilité des flux applicatifs aux interconnexions (URL sur un relai HTTP, en-têtes des messages sur un relai SMTP, etc.) ;

Afin de pouvoir corréler les évènements entre les différents composants, leur source de synchronisation de temps (grâce au protocole NTP) doit être identique.

/RENFORCÉ

Si toutes les actions précédentes ont été mises en œuvre, une centralisation des journaux sur un dispositif dédié pourra être envisagée. Cela permet de faciliter la recherche automatisée d'événements suspects, d'archiver les journaux sur une longue durée et d'empêcher un attaquant d'effacer d'éventuelles traces de son passage sur les équipements qu'il a compromis.

ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, note technique, décembre 2013

37 Définir et appliquer une politique de sauvegarde des composants critiques

/STANDARD

Suite à un incident d'exploitation ou en contexte de gestion d'une intrusion, la disponibilité de sauvegardes conservées en lieu sûr est indispensable à la poursuite de l'activité. Il est donc fortement recommandé de formaliser une politique de sauvegarde régulièrement mise à jour. Cette dernière a pour objectif de définir des exigences en matière de sauvegarde de l'information, des logiciels et des systèmes.

Cette politique doit au moins intégrer les éléments suivants :

- la liste des données jugées vitales pour l'organisme et les serveurs concernés ;
- les différents types de sauvegarde (par exemple le mode hors ligne) ;
- la fréquence des sauvegardes ;
- la procédure d'administration et d'exécution des sauvegardes ;
- les informations de stockage et les restrictions d'accès aux sauvegardes ;
- les procédures de test de restauration ;
- la destruction des supports ayant contenu les sauvegardes.

Les tests de restauration peuvent être réalisés de plusieurs manières :

- systématique, par un ordonnanceur de tâches pour les applications importantes ;
- ponctuelle, en cas d'erreur sur les fichiers ;
- générale, pour une sauvegarde et restauration entières du système d'information.

/RENFORCÉ

Un fois cette politique de sauvegarde établie, il est souhaitable de planifier au moins une fois par an un exercice de restauration des données et de conserver une trace technique des résultats.

38 Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées

/RENFORCÉ

La réalisation d'audits réguliers (au moins une fois par an) du système d'information est essentielle car elle permet d'évaluer concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps. Ces contrôles et audits permettent également de mesurer les écarts pouvant persister entre la règle et la pratique.

Ils peuvent être réalisés par d'éventuelles équipes d'audit internes ou par des sociétés externes spécialisées. Selon le périmètre à contrôler, des audits techniques et/ou organisationnels seront effectués par les professionnels mobilisés. Ces audits sont d'autant plus nécessaires que l'entité doit être conforme à des réglementations et obligations légales directement liées à ses activités.

À l'issue de ces audits, des actions correctives doivent être identifiées, leur application planifiée et des points de suivi organisés à intervalles réguliers. Pour une plus grande efficacité, des indicateurs sur l'état d'avancement du plan d'action pourront être intégrés dans un tableau de bord à l'adresse de la direction.

Si les audits de sécurité participent à la sécurité du système d'information en permettant de mettre en évidence d'éventuelles vulnérabilités, ils ne constituent jamais une preuve de leur absence et ne dispensent donc pas d'autres mesures de contrôle.

Les prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés par l'ANSSI délivrent des prestations d'audit d'architecture, de configuration, de code source, de tests d'intrusion et d'audit organisationnel et physique.

39 Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel

/STANDARD

Toute entité doit disposer d'un référent en sécurité des systèmes d'information qui sera soutenu par la direction ou par une instance décisionnelle spécialisée selon le niveau de maturité de la structure.

Ce référent devra être connu de tous les utilisateurs et sera le premier contact pour toutes les questions relatives à la sécurité des systèmes d'information :

- définition des règles à appliquer selon le contexte ;
- vérification de l'application des règles ;
- sensibilisation des utilisateurs et définition d'un plan de formation des acteurs informatiques ;
- centralisation et traitement des incidents de sécurité constatés ou remontés par les utilisateurs.

Ce référent devra être formé à la sécurité des systèmes d'information et à la gestion de crise.

Dans les entités les plus importantes, ce correspondant peut être désigné pour devenir le relais du RSSI. Il pourra par exemple signaler les doléances des utilisateurs et identifier les thématiques à aborder dans le cadre des sensibilisations, permettant ainsi d'élever le niveau de sécurité du système d'information au sein de l'organisme.

40 Définir une procédure de gestion des incidents de sécurité

/STANDARD

Le constat d'un comportement inhabituel de la part d'un poste de travail ou d'un serveur (connexion impossible, activité importante, activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation, multiples alertes de l'antivirus, etc.) peut alerter sur une éventuelle intrusion.

Une mauvaise réaction en cas d'incident de sécurité peut faire empirer la situation et empêcher de traiter correctement le problème. Le bon réflexe est de déconnecter la machine du réseau, pour stopper l'attaque. En revanche, il faut la maintenir sous tension et ne pas la redémarrer, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque. Il faut ensuite prévenir la hiérarchie, ainsi que le référent en sécurité des systèmes d'information.

Celui-ci peut prendre contact avec un prestataire de réponse aux incidents de sécurité (PRIS) afin de faire réaliser les opérations techniques nécessaires (copie physique du disque, analyse de la mémoire, des journaux et d'éventuels codes malveillants, etc.) et de déterminer si d'autres éléments du système d'information ont été compromis. Il s'agira également d'élaborer la réponse à apporter afin de supprimer d'éventuels codes malveillants et accès dont disposerait l'attaquant et de procéder au changement des mots de passe compromis. Tout incident doit être consigné dans un registre centralisé. Une plainte pourra également être déposée auprès du service judiciaire compétent.

Les prestataires de réponse aux incidents de sécurité (PRIS) interviennent lorsqu'une concordance de signaux permet de soupçonner ou d'attester une activité informatique malveillante au sein d'un système d'information. La criticité de ces prestations engageant la pérennité des systèmes d'information, l'ANSSI a élaboré un référentiel dont l'objectif est d'apporter aux commanditaires de telles prestations les garanties nécessaires vis-à-vis de ces prestataires, tant en termes de compétence que de confiance.

X

POUR ALLER PLUS LOIN

41 Mener une analyse de risques formelle

/RENFORCÉ

Chaque entité évolue dans un environnement informationnel complexe qui lui est propre. Aussi, toute prise de position ou plan d'action impliquant la sécurité du système d'information doit être considéré à la lumière des risques pressentis par la direction. En effet, qu'il s'agisse de mesures organisationnelles ou techniques, leur mise en œuvre représente un coût pour l'entité qui nécessite de s'assurer qu'elles permettent de réduire au bon niveau un risque identifié.

Dans les cas les plus sensibles, l'analyse de risque peut remettre en cause certains choix passés. Ce peut notamment être le cas si la probabilité d'apparition d'un événement et ses conséquences potentielles s'avèrent critiques pour l'entité et qu'il n'existe aucune action préventive pour le maîtriser.

La démarche recommandée consiste, dans les grandes lignes, à définir le contexte, apprécier les risques et les traiter. L'évaluation de ces risques s'opère généralement selon deux axes : leur probabilité d'apparition et leur gravité. S'ensuit l'élaboration d'un plan de traitement du risque à faire valider par une autorité désignée à plus haut niveau.

Trois types d'approches peuvent être envisagés pour maîtriser les risques associés à son système d'information :

> le recours aux bonnes pratiques de sécurité informatique ;
> une analyse de risques systématique fondée sur les retours d'expérience des utilisateurs ;
> une gestion structurée des risques formalisée par une méthodologie dédiée.

Dans ce dernier cas, la méthode EBIOS référencée par l'ANSSI est recommandée. Elle permet d'exprimer les besoins de sécurité, d'identifier les objectifs de sécurité et de déterminer les exigences de sécurité.

La méthode d'analyse de risques EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI.

42 Privilégier l'usage de produits et de services qualifiés par l'ANSSI

/RENFORCÉ

La qualification prononcée par l'ANSSI offre des garanties de sécurité et de confiance aux acheteurs de solutions listées dans les catalogues de produits et de prestataires de service qualifiés que publie l'agence.

Au-delà des entités soumises à réglementation, l'ANSSI encourage plus généralement l'ensemble des entreprises et administrations françaises à utiliser des produits qu'elle qualifie, seul gage d'une étude sérieuse et approfondie du fonctionnement technique de la solution et de son écosystème.

S'agissant des prestataires de service qualifiés, ce label permet de répondre aux enjeux et projets de cybersécurité pour l'ensemble du tissu économique français que l'ANSSI ne saurait adresser seule. Évalués sur des critères techniques et organisationnels, les prestataires qualifiés couvrent l'essentiel des métiers de la sécurité des systèmes d'information. Ainsi, en fonction de ses besoins et du maillage national, une entité pourra faire appel à un Prestataire d'audit de la sécurité des systèmes d'information (PASSI), un Prestataire de réponse aux incidents de sécurité (PRIS), un Prestataire de détection des incidents de sécurité (PDIS) ou à un prestataire de service d'informatique en nuage (SecNumCloud).

Catalogue des produits et prestataires de service qualifiés

I - Sensibiliser et former		STANDARD	RENFORCÉ
1	Former les équipes opérationnelles à la sécurité des systèmes d'information		
2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique		
3	Maîtriser les risques de l'infogérance		

II - Connaitre le système d'information		STANDARD	RENFORCÉ
4	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau		
5	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour		
6	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs		
7	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés		

III - Authentifier et contrôler les accès		STANDARD	RENFORCÉ
8	Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur		
9	Attribuer les bons droits sur les ressources sensibles du système d'information		
10	Définir et vérifier des règles de choix et de dimensionnement des mots de passe		
11	Protéger les mots de passe stockés sur les systèmes		
12	Changer les éléments d'authentification par défaut sur les équipements et services		
13	Privilégier lorsque c'est possible une authentification forte		

IV - Sécuriser les postes		STANDARD	RENFORCÉ
14	Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique		
15	Se protéger des menaces relatives à l'utilisation de supports amovibles		
16	Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité		

17	Activer et configurer le pare-feu local des postes de travail		
18	Chiffrer les données sensibles transmises par voie Internet		

V - Sécuriser le réseau		STANDARD	RENFORCÉ
19	Segmenter le réseau et mettre en place un cloisonnement entre ces zones		
20	S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages		
21	Utiliser des protocoles sécurisés dès qu'ils existent		
22	Mettre en place une passerelle d'accès sécurisé à Internet		
23	Cloisonner les services visibles depuis Internet du reste du système d'information		
24	Protéger sa messagerie professionnelle		
25	Sécuriser les interconnexions réseau dédiées avec les partenaires		
26	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques		

VI - Sécuriser l'administration		STANDARD	RENFORCÉ
27	Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information		
28	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information		
29	Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail		

VII - Gérer le nomadisme		STANDARD	RENFORCÉ
30	Prendre des mesures de sécurisation physique des terminaux nomades		
31	Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable		
32	Sécuriser la connexion réseau des postes utilisés en situation de nomadisme		
33	Adopter des politiques de sécurité dédiées aux terminaux mobiles		

VIII - Maintenir à jour le système d'information		STANDARD	RENFORCÉ
34	Définir une politique de mise à jour des composants du système d'information		
35	Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles		

IX - Superviser, auditer, réagir		STANDARD	RENFORCÉ
36	Activer et configurer les journaux des composants les plus importants		
37	Définir et appliquer une politique de sauvegarde des composants critiques		
38	Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées		
39	Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel		
40	Définir une procédure de gestion des incidents de sécurité		

X - Pour aller plus loin		STANDARD	RENFORCÉ
41	Mener une analyse de risques formelle		
42	Privilégier l'usage de produits et de services qualifiés par l'ANSSI		

Guides et méthodes

ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*, guide, février 2015
www.ssi.gouv.fr/guide-bonnes-pratiques/

ANSSI, *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*, méthode, janvier 2010
www.ssi.gouv.fr/ebios/

ANSSI, *Guide de l'externalisation – Maîtriser les risques de l'infogérance*, guide, décembre 2010
www.ssi.gouv.fr/externalisation/

ANSSI, *Maîtriser les risques de l'infogérance*, guide, décembre 2010
www.ssi.gouv.fr/infogerance/

ANSSI-CDSE, *Passeport de conseils aux voyageurs*, bonnes pratiques, janvier 2010
www.ssi.gouv.fr/passeport-de-conseils-aux-voyageurs/

ANSSI, *Charte d'utilisation des moyens informatiques et des outils numériques – Guide d'élaboration en 8 points clés pour les PME et ETI*, guide, juin 2017
www.ssi.gouv.fr/charte-utilisation-outils-numeriques/

Notes techniques

ANSSI, *Guide de définition d'une architecture de passerelle d'interconnexion sécurisée*, note technique, décembre 2011
www.ssi.gouv.fr/passerelle-interconnexion/

ANSSI, *Recommandations de sécurité relatives aux mots de passe*, note technique, juin 2012
www.ssi.gouv.fr/mots-de-passe/

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013
www.ssi.gouv.fr/politique-filtrage-parefeu/

ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi*, note technique, septembre 2013
www.ssi.gouv.fr/nt-wifi/

ANSSI, *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*, note technique, décembre 2013
www.ssi.gouv.fr/windows-restrictions-logicielles/

ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, note technique, décembre 2013
www.ssi.gouv.fr/journalisation/

ANSSI, *Recommandations de sécurité relatives à Active Directory*, note technique, septembre 2014
www.ssi.gouv.fr/Active-Directory/

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, février 2015
www.ssi.gouv.fr/securisation-admin-si/

ANSSI, *Recommandations de sécurité relatives aux ordiphones*, note technique, juillet 2015
www.ssi.gouv.fr/securisation-ordiphones/

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, note technique, août 2015
www.ssi.gouv.fr/ipsec/

ANSSI, *Recommandations de configuration d'un système GNU/Linux*, note technique, janvier 2016
www.ssi.gouv.fr/reco-securite-systeme-linux/

Ressources en ligne

Site Web de l'ANSSI
Catalogue des produits et prestataires de service qualifiés
www.ssi.gouv.fr/qualifications/

Twitter
@ANSSI_FR
www.twitter.com/anssi_fr

CERT-FR
www.cert.ssi.gouv.fr

CNIL
www.cnil.fr

Références

Douglas Adams, *The Hitchhiker's Guide to the Galaxy* (ou *H2G2*), roman de science-fiction, 1979

Version 2.0 - Septembre 2017

20170901-1756

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr / communication@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

RECOMMANDATIONS RELATIVES À L'INTERCONNEXION D'UN SYSTÈME D'INFORMATION À INTERNET

GUIDE ANSSI

ANSSI-PA-066
18/06/2019

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations relatives à l'interconnexion d'un système d'information à Internet** ». Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence ouverte v2.0 » publiée par la mission Etalab [19].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Ces recommandations n'ont pas de caractère normatif, elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	08/12/2011	Version initiale N°3248/ANSSI/ACE
2.0	18/06/2019	Refonte du plan, ajout d'un chapitre sur l'accès aux contenus Web, nouveau modèle de guide ANSSI

Table des matières

1
Préambule

1.1 Périmètre du guide

Ce guide de l'ANSSI a pour objectif de fournir des recommandations d'architecture technique pour l'interconnexion d'un système d'information (SI) d'une entité – publique ou privée – avec un réseau public. Il peut ainsi être considéré comme une mise à jour étoffée du guide de définition d'une architecture de passerelle d'interconnexion sécurisée [14] publié par l'ANSSI en décembre 2011.

Comme dans la première version, le postulat est que le réseau public interconnecté est Internet car il s'agit du cas le plus fréquent. Il peut y avoir transposition à d'autres contextes, par exemple l'interconnexion au réseau d'un partenaire. Le guide traite aussi bien des flux sortants que des flux entrants vis-à-vis du SI de l'entité.

Ce guide contient le socle nécessaire à la construction de l'interconnexion (chapitres 2 et 3). Des compléments sur les fonctions de sécurité de services applicatifs sont fournis ensuite (chapitre 4 sur l'accès aux contenus hébergés sur le Web). Des recommandations complémentaires pour d'autres services (ex : messagerie, DNS) pourront être publiées dans des guides dédiés ou à l'occasion d'une mise à jour de ce guide.

Attention

Les SI interconnectés avec Internet sont réputés héberger des données publiques ou non sensibles.
Pour les SI hébergeant des données sensibles ou à *Diffusion Restreinte* (DR) au sens de l'II 901 [17], l'application des recommandations de ce guide est nécessaire [1] mais non suffisante. Les lecteurs sont invités à se référer à la réglementation [17] dans l'attente de toute autre publication de l'ANSSI.
Les SI hébergeant des données classifiées de défense au sens de l'IGI 1300 [15] requièrent des passerelles multi-niveaux qui dépassent le cadre de ce guide ; ils ne sont donc pas traités ici.

Ce guide s'adresse à un public technique disposant de connaissances basiques d'architecture réseau et capable d'adapter les recommandations en fonction de ses contraintes et de ses enjeux.

1.2 Convention de lecture

Pour certaines recommandations, il est proposé plusieurs solutions d'architecture qui se distinguent par leur niveau de sécurité. Le lecteur a ainsi la possibilité de choisir une solution en adéquation

1. Les recommandations de type R- (cf. section 1.2) sont fortement déconseillées dans le cas des SI sensibles ou DR. Au contraire, les recommandations de type R* sont fortement conseillées pour ces SI.

avec ses besoins de sécurité.

En outre, dans une démarche itérative de sécurisation, ces différents niveaux de sécurité proposés peuvent permettre de fixer une cible d'architecture et d'identifier les étapes pour l'atteindre.

Ainsi, les recommandations sont présentées de la manière suivante :

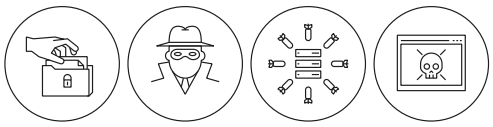
- R*x* constitue une recommandation à l'état de l'art ;
- R*x* - constitue une recommandation alternative à R*x*, d'un niveau de sécurité moindre ;
- R*y* * constitue une recommandation pour les entités ayant des objectifs de sécurité élevés.

Par ailleurs, dans ce guide, l'utilisation du verbe « *devoir* » est volontairement plus prescriptive que la formulation « *il est recommandé* ».

1.3 Menaces considérées

Pour de nombreuses entités, l'interconnexion de leur SI avec Internet est nécessaire, tant ce dernier offre une richesse de services et d'opportunités numériques. Néanmoins il constitue aussi, de manière incontestable aujourd'hui, une source de menaces. Parmi les plus courantes, il est possible de citer :

- l'exfiltration de données depuis le SI de l'entité vers Internet, portant atteinte à leur confidentialité ;
- l'intrusion pour porter atteinte à l'intégrité ou la disponibilité du SI de l'entité ;
- l'usurpation d'identité en accédant à des ressources de l'entité pour rebondir et mener des attaques vers d'autres cibles ;
- le déni de service pour nuire à la disponibilité de l'accès Internet et donc à la productivité ou à l'image de l'entité ;
- l'accès par les collaborateurs à des sites Web interdits par la charte d'utilisation interne voire par la loi.



Si l'accroissement de l'externalisation de services et, potentiellement, du patrimoine informationnel de l'entité dans le nuage (*cloud*) – qui n'est pas le sujet de ce guide – est une réalité, il ne doit pas faire oublier que l'accès à ces services est d'autant plus critique et doit être sécurisé. La performance et la disponibilité de l'accès à Internet peuvent devenir aussi critiques que l'accès au réseau privé de l'entité.

1.4 Hygiène informatique et pré-requis

Dans le guide d'hygiène informatique [3] publié par l'ANSSI en 2017, le déploiement d'une passerelle sécurisée d'accès à Internet fait l'objet d'une mesure spécifique (mesure 22) ; ce guide en est une déclinaison.

Afin de ne pas surcharger ce guide et de se concentrer sur les recommandations spécifiques au contexte, les lecteurs sont invités à se référer au guide d'hygiène informatique pour en appliquer les mesures élémentaires, dont notamment :

- former les équipes opérationnelles afin que celles-ci maîtrisent les solutions déployées ;
- maintenir une cartographie, précisant notamment les points d'interconnexion avec Internet ;
- segmenter le SI en zones homogènes ;
- maîtriser les risques de l'infogérance en cas d'externalisation ;
- définir une politique de mise à jour ;
- activer et configurer les journaux des composants les plus importants.

1.5 Expression du besoin

En premier lieu, il est indispensable d'identifier clairement et formellement les besoins métier liés à Internet, pour construire et sécuriser l'architecture technique d'interconnexion spécifique à l'entité. Pour les phases ultérieures, ce travail préliminaire doit faciliter l'établissement de matrices de flux et de règles de contrôles d'accès.

Information

Dans ce guide, on convient qu'un *flux* désigne un flux de données, reposant généralement sur IP, pouvant être transporté sur TCP ou UDP et ayant un sens (entrant ou sortant) vis-à-vis d'Internet ou du SI de l'entité.

R1

Déterminer l'ensemble des services nécessitant l'interconnexion à Internet

Afin de déployer une infrastructure d'interconnexion répondant au juste besoin fonctionnel de l'entité, il est nécessaire d'établir de manière exhaustive une liste des services du SI de l'entité (applications métier, services d'infrastructure) nécessitant une interconnexion à Internet, en distinguant les flux entrants et les flux sortants.
Cette liste doit être mise à jour dès que nécessaire et revue régulièrement.

À titre d'exemple, voici une liste non exhaustive de services nécessitant une interconnexion à Internet :

- la navigation Web ;
- la récupération de sources ou de mises à jour logicielles depuis des sites de confiance ;
- la résolution de noms DNS publics ;
- les services publics de l'entité exposés sur Internet (ex : hébergements Web, DNS publics) ;
- les services d'infrastructures de l'entité exposés sur Internet (ex : passerelle VPN IPsec ou TLS pour les accès nomades, passerelle VPN IPsec pour des tunnels site à site) ;
- les services collaboratifs de l'entité exposés sur Internet (ex : messagerie, téléphonie, visioconférence, portail Extranet) ;

- les services métier de l'entité exposés sur Internet (ex : EDI [2]) ;
- l'accès à Internet pour les visiteurs.

Information

La mise en œuvre de passerelles VPN pour les accès nomades est traitée de manière détaillée dans le guide de l'ANSSI sur le nomadisme numérique [13] en cohérence avec la doctrine de ce guide plus générique.

Par ailleurs, la conception d'une passerelle d'interconnexion ne se limite pas au choix d'un boîtier (ou *appliance*) multi-services sur étagère. Elle nécessite en premier lieu l'identification des fonctions de sécurité à mettre en œuvre sur l'interconnexion et de leur position dans l'architecture. Le choix de chaque équipement constituant la passerelle doit se faire sur la base de trois critères :

- son apport sur le plan de la sécurité ;
- sa robustesse ;
- la capacité pour l'équipe technique chargée de le mettre en œuvre de le maîtriser et de le maintenir dans un état sécurisé.

À cet effet, s'agissant de la robustesse, l'emploi de produits disposant d'un visa de sécurité [3] de l'ANSSI est recommandé.

2. Échange de données informatisées.
3. https://www.ssi.gouv.fr/visa-de-securite.

2
Architecture et fonctions de sécurité de l'interconnexion

2.1 Précisions sur le concept de zone démilitarisée

En informatique, le concept militaire de *zone démilitarisée* (DMZ [4]) est régulièrement réutilisé pour désigner un sous-réseau (concrètement, quelques équipements) séparant deux zones de confiance hétérogène notamment grâce à des pare-feux réalisant un filtrage périmétrique de part et d'autre (cf. figure 2.1).

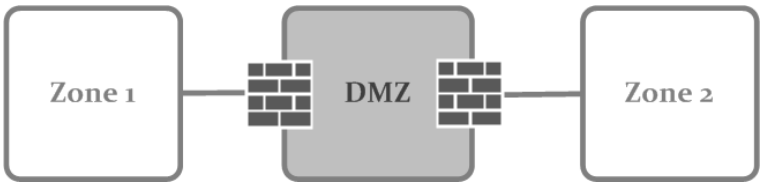


FIGURE 2.1 – Zone démilitarisée

Dans le cas d'une interconnexion à Internet au moyen d'une DMZ, différents points de filtrage et d'analyse du trafic sont également nécessaires pour traiter les risques liés aux menaces identifiées (cf. section 1.3). Pour cela, il convient donc de limiter tout accès direct qui serait simplement routé entre le SI de l'entité et Internet. Concrètement, la DMZ disposant d'un filtrage périmétrique, d'une part avec Internet et d'autre part avec le SI de l'entité, doit également intégrer, autant que nécessaire, des relais applicatifs implémentant des fonctions de sécurité (ex : serveur mandataire – *proxy* – pour les accès Web, résolveur DNS pour les requêtes de noms DNS publics).

De plus, la DMZ est ici considérée comme une zone neutre et perdable. En effet, sa sensibilité n'est pas nulle (des données du SI de l'entité peuvent y être exposées ou au moins y transiter) mais une attaque en intégrité ou en confidentialité sur ses composants ne doit pas remettre en cause de manière irréversible et durable le bon fonctionnement du SI de l'entité. À titre d'exemple, la compromission d'un relais de messagerie au sein d'une DMZ pourrait amener à décider sa destruction et sa reconstruction sans que les boîtes de messagerie hébergées et protégées de manière *ad hoc* dans le SI de l'entité ne soient elles-mêmes détruites.

4. L'acronyme anglais DMZ pour *demilitarized zone* est le plus couramment utilisé.

Passerelle d'interconnexion sécurisée

Une passerelle d'interconnexion sécurisée est constituée d'une ou plusieurs « DMZ » qui doivent être des zones neutres, perdables, protégées par des pare-feux périmétriques et servant, en leur sein et autant que possible, à la rupture protocolaire et à l'analyse du trafic échangé entre un réseau public et le SI de l'entité.

Pour la suite du guide, on convient de parler de *passerelle Internet sécurisée*. De plus, dans un souci de simplification, on convient de parler de *la* DMZ constituant la passerelle Internet sécurisée dans les principes d'architecture générale. Elle sera utilement décomposée en plusieurs DMZ dans les principes d'architecture détaillée (section 2.4).

2.2 Filtrage et cloisonnement

2.2.1 Filtrage périmétrique et filtrage interne

Le fournisseur d'accès à Internet (FAI) de l'entité propose généralement son service en positionnant un routeur d'accès (éventuellement appelé *box* pour les plus petits modèles intégrés) dans les locaux de l'entité. Cet équipement est sous responsabilité du FAI. Même s'il est présenté comme embarquant des fonctions de sécurité, c'est avant tout un équipement réseau de routage et non un équipement de sécurité. Afin de maîtriser la sécurité périmétrique du SI de l'entité, celle-ci doit mettre en œuvre un premier niveau de filtrage IP sous son contrôle et indépendant du routeur d'accès (cf. figure 2.2).

R2

Déployer un pare-feu maîtrisé entre la DMZ et le routeur d'accès Internet

L'interconnexion entre Internet et la DMZ doit être protégée de façon périmétrique par une fonction de filtrage IP assurée par un pare-feu. Ce dernier est dit *externe* ; il doit être maîtrisé par l'entité (ou un prestataire mandaté à cet effet) et ne doit pas être contournable.
Une matrice des flux correspondant au juste besoin opérationnel doit être définie, mise en œuvre sur ce pare-feu et revue régulièrement.

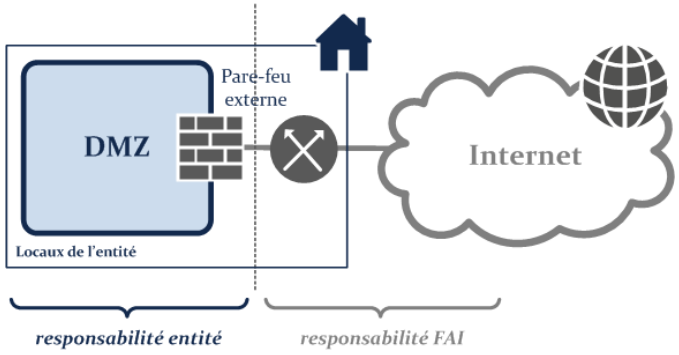


FIGURE 2.2 – Filtrage périmétrique avec Internet grâce à un pare-feu externe

Seules les ressources (ex : postes de travail, serveurs) ayant un besoin opérationnel légitime de connexion à Internet doivent être autorisées à y accéder. Un découpage du SI de l'entité en zones homogènes, amenant à un adressage en sous-réseaux IP distincts, doit permettre de déterminer quelles sont les zones autorisées à accéder à la passerelle Internet sécurisée. Une fonction de filtrage doit dès lors être mise en œuvre entre le SI de l'entité et la DMZ (cf. figure 2.3).

R3

Déployer un pare-feu maîtrisé entre le SI de l'entité et la DMZ

L'interconnexion entre le SI de l'entité et la DMZ doit être protégée de façon périmétrique par une fonction de filtrage IP assurée par un pare-feu. Ce dernier est dit *interne* ; il doit être maîtrisé par l'entité (ou un prestataire mandaté à cet effet) et ne doit pas être contournable.
Une matrice des flux correspondant au juste besoin opérationnel doit être définie, mise en œuvre sur ce pare-feu et revue régulièrement.

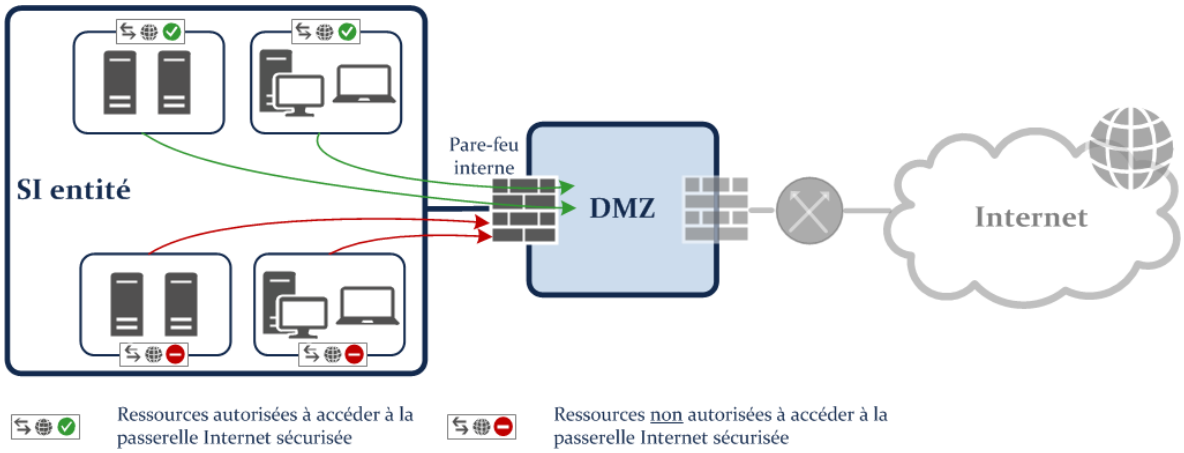


FIGURE 2.3 – Filtrage périmétrique avec le SI de l'entité grâce à un pare-feu interne

Information

Pour la suite du guide, la *passerelle Internet sécurisée* inclut la DMZ d'interconnexion entre le SI de l'entité et Internet ainsi que les pare-feux périmétriques qui la protègent. Celle-ci est ainsi représentée sur la figure 2.4.

R4

Rendre incontournable la passerelle Internet sécurisée

Tout système d'information nécessitant une interconnexion avec Internet doit être protégé par une passerelle Internet sécurisée mettant en œuvre au minimum des fonctions de filtrage périmétrique ainsi que des services applicatifs relais.
Cette passerelle doit être incontournable. En particulier, tout autre accès à Internet pour des besoins spécifiques, potentiellement non compatibles avec la passerelle (ex : accès Internet à des fins de test « comme à la maison », sans aucune fonction de sécurité depuis un poste dédié) doit être réalisé depuis des infrastructures physiquement distinctes.

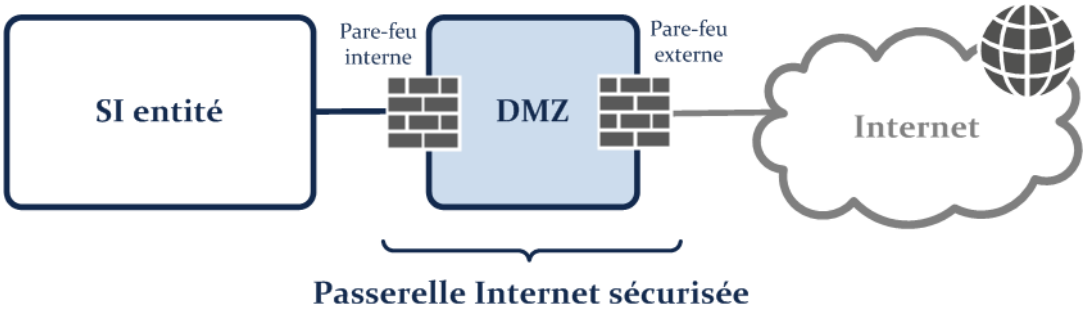


FIGURE 2.4 – Interconnexion du SI de l'entité et d'Internet au moyen d'une passerelle Internet sécurisée

Information

D'ores et déjà, il convient de préciser que les pare-feux interne et externe doivent être physiquement distincts dans une démarche de défense en profondeur. Plus de détails sont fournis dans le paragraphe 2.4.4.
Par ailleurs, s'agissant de la question de la diversification technologique des pare-feux interne et externe et des niveaux de visas de sécurité recommandés, le guide [11] de l'ANSSI est dédié à ce sujet ; le lecteur est invité à s'y référer.
Enfin, l'ANSSI publie également des recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu [5] et pour son nettoyage [10].

Dans le cas où certains services applicatifs sont directement hébergés au sein de la passerelle Internet sécurisée (ex : hébergement d'un serveur Web), il est souhaitable de filtrer les flux entre les serveurs métier (ex : serveur Web) et les serveurs relais applicatifs (ex : serveur mandataire inverse – *reverse proxy*). Dans ce cas, un ou plusieurs pare-feux dit *intermédiaires* sont déployés en coupure pour assurer le filtrage (cf. figures 2.13 et 2.15).

R5

Déployer si nécessaire des pare-feux intermédiaires dans la passerelle Internet sécurisée

Afin de filtrer les flux internes de la passerelle Internet sécurisée entre des serveurs métier et des serveurs relais, la mise en œuvre d'un ou plusieurs pare-feux intermédiaires complémentaires est recommandée.

2.2.2 Cloisonnement et cinématique des flux

Des flux très hétérogènes peuvent transiter par la passerelle Internet sécurisée à l'initiative du SI de l'entité vers Internet (services accédés) ou, à l'inverse, des flux à l'initiative d'Internet vers le SI de l'entité (services hébergés). Suivant la confiance accordée à la zone source (généralement plus élevée lorsqu'il s'agit du SI de l'entité que d'Internet) et suivant les besoins de sécurité du service (ex : hébergement d'un simple site Web *versus* accès nomade des administrateurs en VPN IPsec), les mesures de sécurité sont différentes. Dès lors, des chaînes de traitement distinctes doivent être construites et cloisonnées au sein de la passerelle Internet sécurisée ; celles-ci sont constituées par exemple de serveurs relais applicatifs, d'équipements réseau d'accès et de sécurité.

R6

Cloisonner les flux au sein de chaînes de traitement homogène

Afin d'adapter les mesures de sécurité en fonction de la source des flux et des besoins de sécurité du service, autant de chaînes de traitement distinctes doivent être construites et cloisonnées au sein de la passerelle Internet sécurisée.
La nature du cloisonnement, physique de préférence ou logique à défaut, dépend des besoins de sécurité et de l'exposition des services et doit être déterminée par une analyse de risque.

Information

Cette recommandation R6 est volontairement généraliste mais sera déclinée dès que nécessaire par service (ex : accès à la navigation Web *versus* hébergement Web) et est appliquée sur le schéma d'architecture multi-services (cf. figure 2.22 en p. 25).

En outre, il est recommandé que la cinématique des flux vis-à-vis de la passerelle Internet sécurisée respecte des règles simples mais strictes, illustrées par la figure 2.5 :

- tout flux en provenance du SI et à destination d'Internet (accès) est initié par le client du SI vers la passerelle Internet sécurisée puis de la passerelle Internet sécurisée vers Internet ;
- tout flux en provenance d'Internet et à destination du SI (hébergement) est initié par le client sur Internet vers la passerelle Internet sécurisée ; au sein de cette passerelle, les serveurs reçoivent à la fois des flux provenant d'Internet et du SI ; en d'autres termes, il n'y a pas de flux initié depuis la passerelle Internet sécurisée vers le SI.

R7

Respecter une cinématique sécurisée des flux

Le principe d'un flux initié depuis une zone de plus haute confiance vers une zone de moindre confiance doit ici être adapté au contexte d'une passerelle Internet sécurisée, respectivement vis-à-vis d'Internet et du SI de l'entité.
Il est recommandé en particulier de ne pas initier de flux depuis la passerelle Internet sécurisée vers le SI de l'entité.

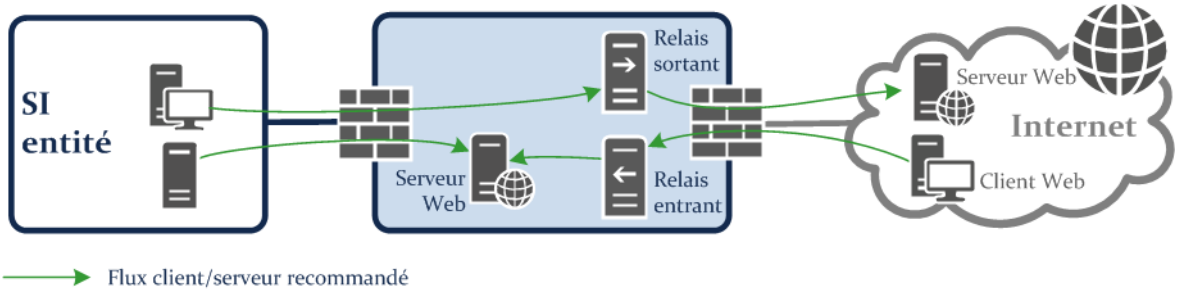


FIGURE 2.5 – Exemple de cinématique sécurisée des flux vis-à-vis de la passerelle Internet sécurisée

La recommandation R7 n'est malheureusement pas applicable à l'ensemble des flux entrants (ex : cas d'un relais entrant de messagerie, cf. figure 2.6). Une alternative, d'un niveau de sécurité moindre, consiste à ce qu'un nombre limité de serveurs puisse initier une connexion vers le SI de l'entité. Dès lors, il est indispensable de bien cloisonner les ressources concernées au sein du SI.

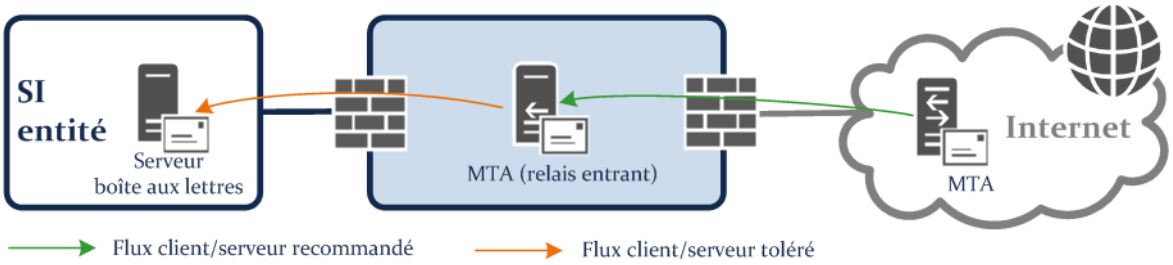


FIGURE 2.6 – Exemple de cinématique alternative et moins sécurisée de flux entrants vis-à-vis de la passerelle Internet sécurisée

2.3 Fonctions de sécurité génériques de l'interconnexion

Au-delà du filtrage au moyen de pare-feux et des principes de cloisonnement, la passerelle Internet sécurisée doit répondre à des besoins de détection afin de réagir au plus tôt en cas d'incident de sécurité et d'authentification à des fins de contrôle d'accès et d'imputabilité.

2.3.1 Détection : rupture protocolaire et analyse de flux

L'interconnexion avec un réseau de moindre confiance (ici Internet) impose à l'entité un principe de base : tout flux entrant ou sortant doit au minimum bénéficier d'une rupture protocolaire afin de ne pas exposer sur Internet la pile IP des ressources de l'entité et, suivant les cas, bénéficier d'une analyse dans l'objectif de détecter une fuite de données ou l'introduction d'un code malveillant.

Rupture protocolaire

Une rupture protocolaire consiste à casser en entrée et reconstruire en sortie la communication entre deux ressources (généralement un client et un serveur) au niveau d'une des couches du modèle OSI [5].
Les protocoles en entrée et en sortie peuvent être distincts suivant les contraintes techniques de l'environnement et les objectifs de sécurité.

R8

Procéder à une rupture protocolaire des flux

Afin de se prémunir de connexions malveillantes directes entre une ressource de l'entité et une ressource sur Internet (ex : un serveur de commande et contrôle), une rupture protocolaire doit être mise en œuvre au sein de la passerelle Internet sécurisée.

R9

Procéder à une analyse des flux en fonction de l'analyse de risque

Pour éviter toute fuite de données ou introduction de codes malveillants, une analyse des flux est recommandée lors de cette rupture protocolaire.

5. *Open System Interconnections*.

Attention

Cette recommandation s'applique dès lors qu'au moins une des parties n'est pas de confiance, comme un site Web hébergé sur Internet auquel accède un client de l'entité ou un client Web sur Internet qui accède à un site Web hébergé par l'entité.
Dans le cas de deux points de confiance maîtrisés par l'entité utilisant Internet comme réseau de transport, comme un client VPN déployé sur un poste nomade de l'entité et un concentrateur VPN hébergé par l'entité, la rupture du tunnel VPN n'est pas recommandée afin de préserver la confiance dans la confidentialité, l'intégrité et l'authenticité des flux.

Pour compléter les moyens de détection, l'architecture de la passerelle Internet sécurisée peut également prévoir l'ajout de dispositifs permettant une copie du trafic (*taps* réseau), et de sondes de sécurité pour analyser ce trafic dupliqué. Il est alors recommandé que ces équipements de sécurité disposent d'un visa de sécurité de l'ANSSI. Dans certains cas, la mise en œuvre de ces équipements est imposée par la législation (ex : aux interconnexions pour les SI sensibles au sens de l'II 901 [17] ou pour les systèmes d'information d'importance vitale au sens de la loi de programmation militaire 2013).

2.3.2 Authentification

Pour les besoins d'authentification au sein de la passerelle Internet sécurisée, il est indispensable de ne pas exposer un annuaire hébergé dans le SI de l'entité directement aux équipements de la passerelle Internet sécurisée. En effet, une vulnérabilité d'un de ses équipements pourrait amener à une prise de contrôle de cet annuaire puis du SI de l'entité. Trois solutions d'architecture sont envisageables suivant le niveau de sécurité visé et les méthodes d'authentification permises par les équipements de la passerelle Internet sécurisée :

- un annuaire dédié au sein de la passerelle Internet sécurisée, synchronisé à l'initiative d'un annuaire hébergé sur le SI de l'entité, contenant les données correspondant au strict besoin opérationnel et, sauf contrainte exceptionnelle, en lecture seule (cf. figure 2.7) ; cette solution respecte la cinématique sécurisée des flux (cf. R7) ;
- un serveur mandataire inverse d'authentification (ex : *reverse proxy* LDAP) hébergé au sein de la passerelle Internet sécurisée, configuré avec les restrictions idoines pour des échanges avec un annuaire hébergé sur le SI de l'entité (cf. figure 2.8) ; cette solution évite l'hébergement des données d'authentification dans la passerelle Internet sécurisée mais déroge à la cinématique sécurisée des flux (cf. R7) ;
- pour les flux sortants, un serveur mandataire dédié à l'authentification au sein du SI de l'entité et requêtant un annuaire du SI de l'entité (cf. figure 2.9) ; dans ce cas, aucune authentification n'est nécessaire au sein de la passerelle Internet sécurisée ; c'est la solution la plus sécurisée mais potentiellement coûteuse à déployer et à maintenir.

La réutilisation d'une base d'authentification existante (ex : celle des postes bureautiques) est possible grâce à des mécanismes standards (ex : RADIUS, LDAPS).

R10

Ne pas exposer d'annuaire du SI de l'entité aux ressources de la passerelle Internet sécurisée

En aucun cas un annuaire du SI de l'entité ne doit être directement requêté par les équipements de la passerelle Internet sécurisée pour les besoins propres d'authentification. Trois architectures sont proposées pour y répondre :

- un annuaire dédié, minimaliste et en lecture seule, au sein de la passerelle Internet sécurisée ;
- un serveur mandataire inverse d'authentification au sein de la passerelle Internet sécurisée ;
- un serveur mandataire au sein du SI de l'entité dédié aux besoins d'authentification de la passerelle Internet sécurisée.

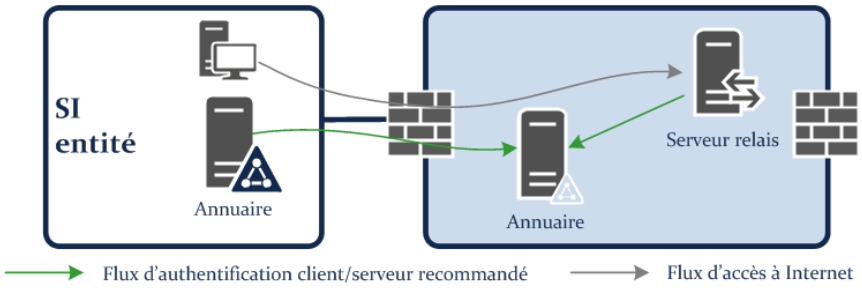


FIGURE 2.7 – Annuaire dédié au sein de la passerelle Internet sécurisée, synchronisé à l'initiative d'un annuaire du SI de l'entité et requêté par un serveur relais applicatif

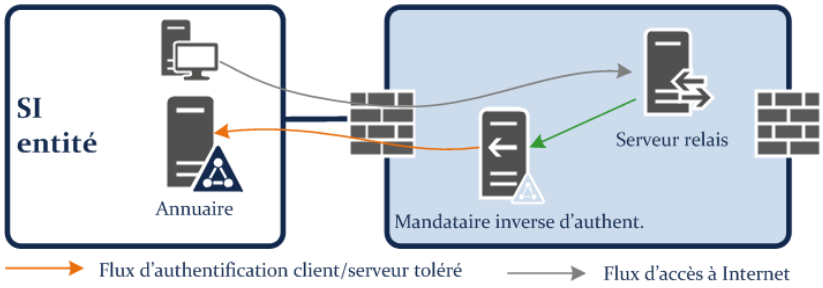


FIGURE 2.8 – Serveur mandataire inverse d'authentification au sein de la passerelle Internet sécurisée, requêtant un annuaire du SI de l'entité et requêté par un serveur relais applicatif

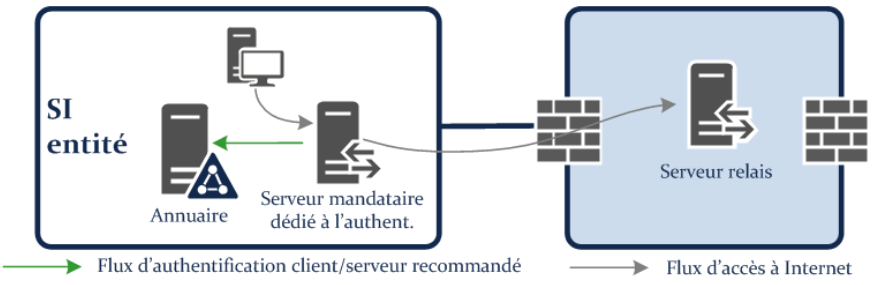


FIGURE 2.9 – Serveur mandataire au sein du SI de l'entité dédié aux besoins d'authentification de la passerelle Internet sécurisée et y transférant les requêtes

2.4 Architecture détaillée

Cette section présente des architectures détaillées d'une passerelle Internet sécurisée classées par niveau de sécurité décroissant. Dans tous les cas, on distingue cinq types de zones (regroupements de ressources logicielles ou matérielles) :

- la *zone d'accès interne* pour le filtrage entre le SI de l'entité et la passerelle Internet sécurisée ;
- la *zone de services internes* pour les ressources dédiées au fonctionnement de la passerelle Internet sécurisée ;
- la *zone de services exposés* pour l'hébergement éventuel [6] de serveurs métier (ex : serveur Web, serveur de transfert de fichiers) ;
- la *zone de services relais* pour la rupture protocolaire et l'analyse des flux ;
- la *zone d'accès externe* pour le filtrage entre la passerelle Internet sécurisée et Internet.

Avant d'aborder les alternatives possibles d'architecture de passerelle Internet sécurisée, une représentation macroscopique de ces zones est proposée sur la figure 2.10.

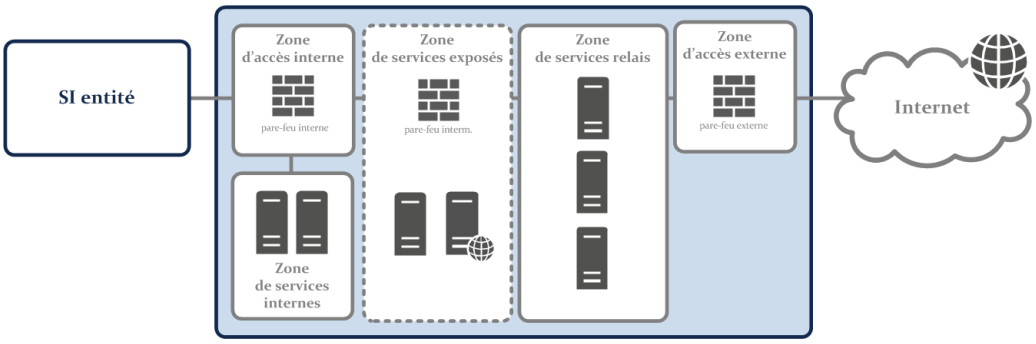


FIGURE 2.10 – Représentation macroscopique des zones d'une passerelle Internet sécurisée

2.4.1 Rappels sur les risques de la mutualisation par virtualisation

Les facilités opérationnelles permises par la mutualisation par virtualisation peuvent inciter à regrouper différentes ressources logicielles (services, applicatifs ou réseau), sur une même ressource physique. Ce regroupement peut consister à exécuter différentes applications sur le même système d'exploitation ou à mettre en œuvre des techniques de virtualisation plus ou moins lourdes.

Dans le contexte de la passerelle Internet sécurisée, les risques liés à la mutualisation des ressources sont les suivants :

- déni de service : le dysfonctionnement d'une des applications installées sur une machine physique peut entraîner une indisponibilité de l'ensemble des services s'exécutant sur la machine ;
- compromission de services : si un attaquant parvient à prendre le contrôle d'un service donné, il lui sera généralement beaucoup plus facile de compromettre les différents services s'exécutant sur la même machine physique (par escalade locale de privilège par exemple ou attaques de plus bas niveau [7]).

6. Cette zone, déployée ou non suivant le contexte, est volontairement représentée en pointillés sur la figure 2.10.
7. Les vulnérabilités Spectre et Meltdown affectant plusieurs familles de processeurs et pouvant conduire à des fuites de données sont deux exemples récents à la date de parution de ce guide. Cf. https ://cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-001/.

L'opportunité d'exécuter sur une même machine plusieurs services doit être évaluée en prenant en compte les recommandations suivantes :

- il est recommandé de n'héberger sur une même machine physique que les ressources d'une même zone (cf. figure 2.11) ;
- il est recommandé de n'héberger sur une même machine que des services identiques d'un point de vue fonctionnel et de la sécurité. Par exemple, il est déconseillé d'exécuter sur la même machine un serveur Web et un *reverse proxy* Web ;
- il est recommandé d'isoler sur une même machine physique les services notoirement moins bien sécurisés ;
- il n'est pas souhaitable d'héberger sur une même machine physique un serveur nominal et son éventuel serveur de secours.

De plus, certaines limitations opérationnelles liées aux éventuelles adhérences des services à un système d'exploitation ou à une architecture matérielle particulière viennent limiter les capacités en matière de mutualisation de services.

R11

Évaluer les risques de mutualisation par virtualisation

Les opportunités permises par la virtualisation doivent être mises au regard des risques qu'elle présente.
Le principe de précaution doit prévaloir : des ressources peuvent être virtualisées et mutualisées sur un socle physique commun à la condition que les services qu'elles portent aient des besoins de sécurité et une exposition homogènes.

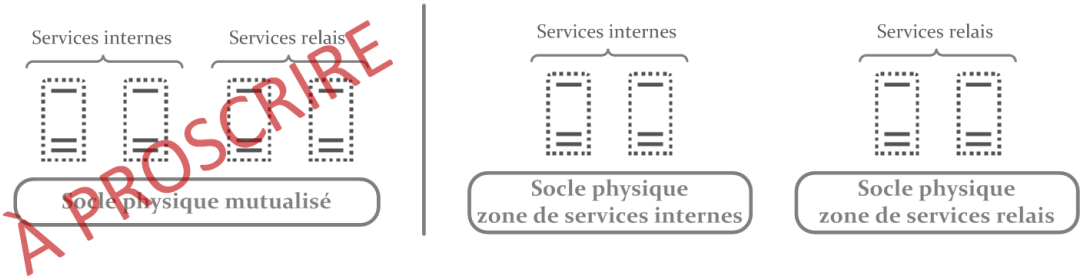


FIGURE 2.11 – Principes de (non) mutualisation par virtualisation

2.4.2 Cas 1 : absence de mutualisation par virtualisation entre zones

La solution ayant le niveau de sécurité le plus élevé consiste à dédier des équipements physiques pour chaque zone y compris pour la commutation (cf. figures 2.12 et 2.13). En effet, la forte exposition des zones d'accès interne et externe incite à ne pas mutualiser des fonctions de filtrage ou de commutation sur un même équipement physique, quand bien même celui-ci permettrait de déployer des instances virtuelles.

R12

Déployer une passerelle Internet sécurisée à base d'équipements physiques dédiés par zone

Afin de garantir le cloisonnement effectif entre chaque zone de la passerelle Internet sécurisée et *in fine* entre le SI de l'entité et Internet, il est recommandé de dédier des équipements physiques par zone, y compris pour le filtrage et la commutation.

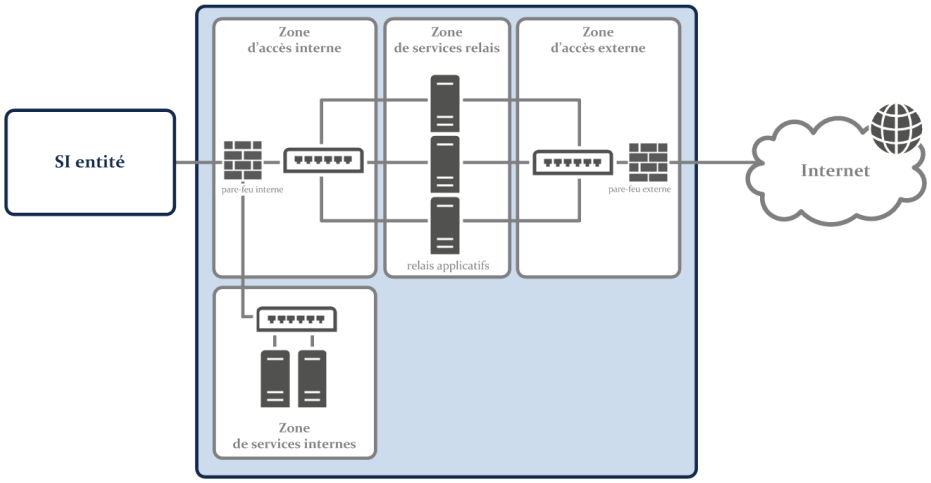


FIGURE 2.12 – Architecture recommandée d'une passerelle Internet sécurisée (sans zone de services exposés)

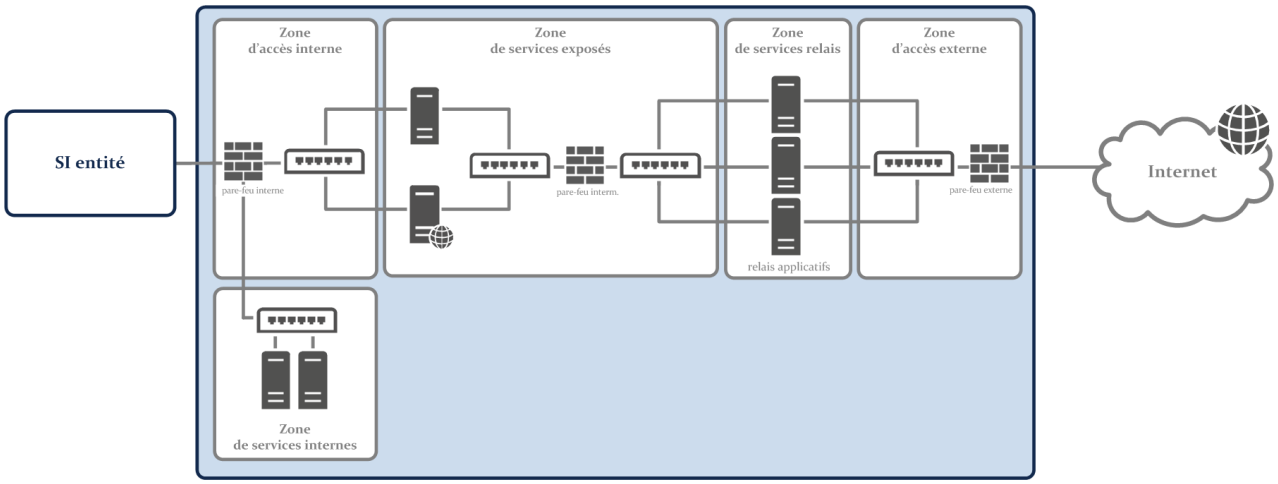


FIGURE 2.13 – Architecture recommandée d'une passerelle Internet sécurisée (avec zone de services exposés)

2.4.3 Cas 2 : mutualisation physique de la commutation

Une solution d'un niveau de sécurité moindre consiste à mutualiser physiquement la commutation au niveau de la zone de services relais (cf. figure 2.14) voire de la zone de services exposés (cf. figure 2.15). Dans ce cas, une segmentation logique doit toutefois être réalisée à l'aide de VLAN (*Virtual Local Area Network*). Le durcissement réalisable sur le commutateur mutualisé est en effet

moindre que celui-ci réalisable sur les serveurs de la zone de services relais (ou de la zone de services exposés) disposant de deux interfaces physiques.

R12 -

Déployer une passerelle Internet en acceptant la mutualisation de certains équipements de commutation

La dérogation à l'architecture la plus sécurisée consiste à mutualiser les équipements de commutation pour les zones d'accès interne, des services relais et d'accès externe de la passerelle Internet sécurisée.
Dans ce cas, des commutateurs physiques dédiés respectivement à la zone de services internes et à l'éventuelle zone de services exposés doivent être maintenus.

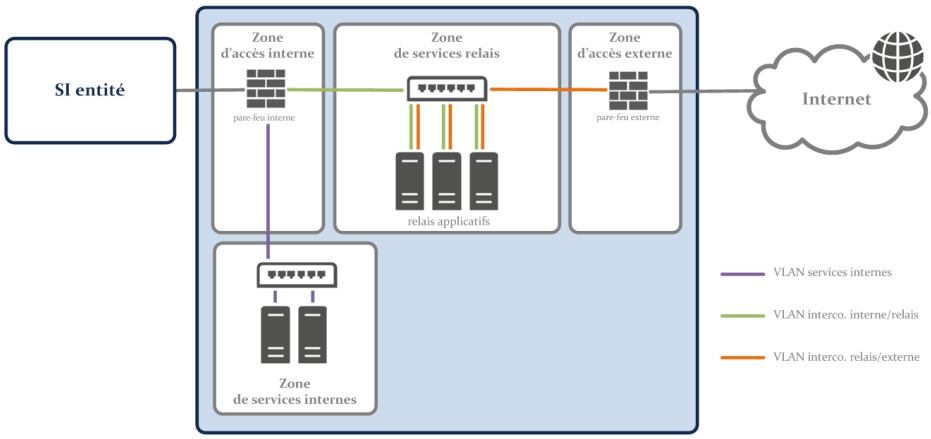


FIGURE 2.14 – Architecture d'une passerelle Internet sécurisée avec mutualisation d'une partie de la commutation (sans zone de services exposés)

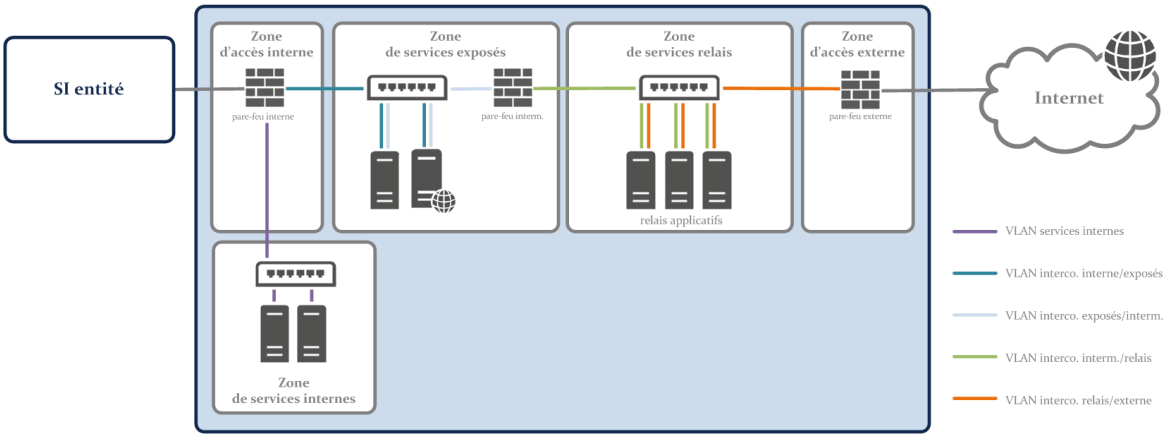


FIGURE 2.15 – Architecture d'une passerelle Internet sécurisée avec mutualisation d'une partie de la commutation (avec zone de services exposés)

Information

L'ANSSI publie un guide de recommandations pour la sécurisation d'un commutateur de desserte [1] qu'il est utile de consulter à cette occasion.

2.4.4 Cas 3 : mutualisation du filtrage à proscrire

Une solution d'un niveau de sécurité moindre consisterait à mutualiser le filtrage de la passerelle Internet sécurisée vers Internet et vers le SI (c'est-à-dire les pare-feux interne et externe) sur un seul équipement physique.

Attention

Il est important de comprendre que, dans cette architecture, la compromission de l'unique pare-feu ou une erreur de configuration peut donner un accès direct entre le SI et Internet, ce dont on cherche à se protéger.

Cette architecture (cf. figure 2.16) n'est pas recommandée. En particulier, elle n'est pas conforme aux exigences de l'II 901 [17] pour les SI sensibles ou *Diffusion Restreinte*.

R13

Proscrire toute mutualisation des pare-feux interne et externe

En raison de la forte exposition des zones d'accès interne et externe, toute mutualisation des pare-feux interne et externe, même à l'aide d'instances virtuelles distinctes déployées sur un socle physique commun, doit être proscrite.

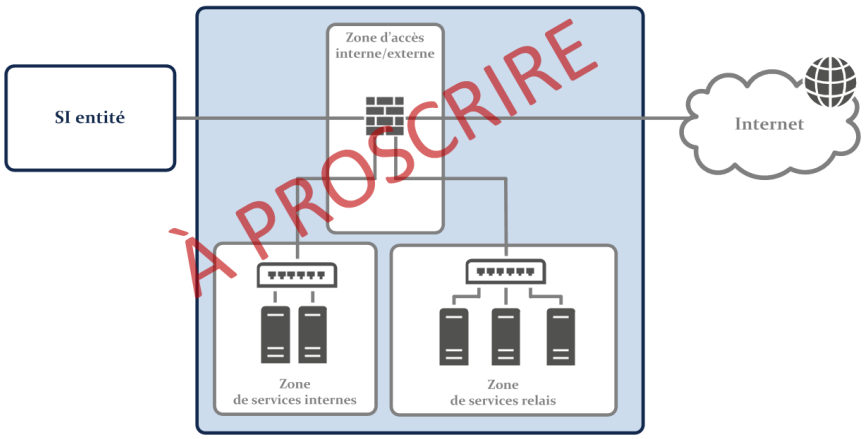


FIGURE 2.16 – Architecture à proscrire d'une passerelle Internet sécurisée avec mutualisation du filtrage

2.4.5 Gestion du cas d'exception des connexions directes

L'architecture recommandée (R12) permet, grâce à une coupure physique, de garantir qu'aucune communication n'est possible entre les pare-feux interne et externe sans passer par la zone de services relais. Sans cette coupure physique – c'est le cas de l'architecture alternative (R12-) – il existe un risque qu'un flux sortant transite directement sans qu'il ne soit filtré au niveau applicatif. Toutefois, certains flux sortants peuvent être difficiles voire impossibles à traiter par un relais applicatif.

En premier recours, il est nécessaire d'étudier avec attention les possibilités de configuration du logiciel client nécessitant un accès à Internet (ex : configuration *proxy* HTTP) et l'ensemble des configurations permises par le relais. Par exemple, l'utilisation de tunnels grâce à la méthode HTTP

CONNECT sur un serveur mandataire HTTP peut répondre à certains cas d'usage. Il convient dès lors d'être extrêmement attentif à la configuration associée du serveur mandataire s'agissant des restrictions d'adresses IP source/destination et de ports TCP destination.

En dernier recours, il peut être nécessaire de raccorder directement les pare-feux externe et interne par un lien physique sans passage par un serveur relais (cf. figure 2.17). Dans ce cas, la gestion des matrices de flux et du routage doit être d'autant plus stricte sur ces deux pare-feux. De plus, seules des zones dédiées du SI de l'entité doivent être autorisées à utiliser ce chemin d'accès ; ces zones doivent apparaître explicitement sur la cartographie du SI et être filtrées suivant le strict besoin opérationnel.

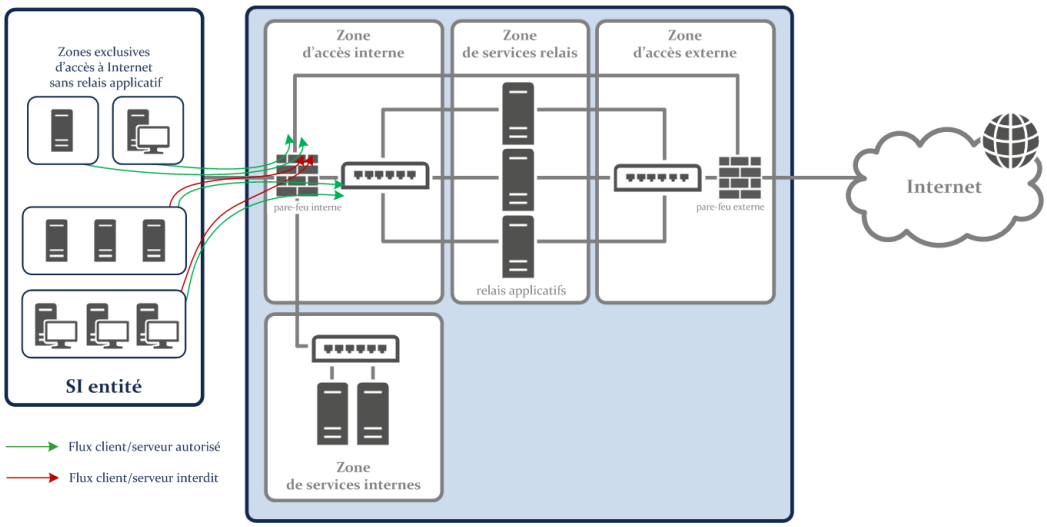


FIGURE 2.17 – Architecture d'une passerelle Internet sécurisée avec lien physique direct entre zones d'accès interne et externe

2.4.6 Cas particulier du DNS

Le protocole DNS permettant la conversion de noms de domaine en adresses IP est aujourd'hui indispensable pour accéder légitimement à des ressources aussi bien sur les réseaux privés que sur Internet. Dans le même temps, il peut constituer un canal privilégié d'exfiltration de données pour un attaquant qui en détournerait l'usage initial. Par exemple, cela peut être mis en œuvre après activation d'une charge malveillante (par hameçonnage, piégeage de clé USB…) depuis une ressource (poste de travail ou serveur) connectée à Internet. Il est donc indispensable de bloquer toute possibilité technique d'établir un canal DNS direct (ou indirect) depuis une ressource du SI de l'entité vers Internet.

Si l'exhaustivité des recommandations relatives à une architecture DNS n'est pas l'objet de ce guide, il convient d'évoquer celles nécessaires à la compréhension des choix d'architecture recommandés pour une passerelle Internet sécurisée :

- des résolveurs DNS doivent être dédiés dans le SI de l'entité pour les résolutions de noms DNS internes (adressage privé de l'entité) ;
- des résolveurs DNS doivent être dédiés dans la passerelle Internet sécurisée pour les résolutions de noms DNS publics (adressage sur Internet) ;

- les résolveurs pré-cités ne doivent pas communiquer entre eux ;
- les ressources du SI de l'entité (postes de travail, serveurs) ne doivent adresser leurs requêtes de noms DNS internes qu'aux résolveurs DNS internes ; en conséquence le pare-feu interne doit par défaut bloquer tous les flux DNS ;
- les relais de la passerelle Internet sécurisée ne doivent adresser les requêtes de noms DNS publics qu'aux résolveurs DNS publics.

Ces recommandations sont représentées sur la figure 2.18.

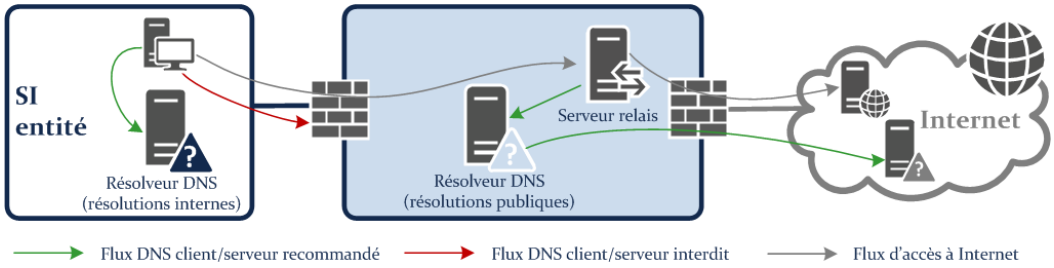


FIGURE 2.18 – Cinématique des flux DNS

2.5 Raccordement des sites géographiques

Pour une entité disposant de plusieurs sites géographiques reliés par un réseau privé étendu (WAN [8]), il est possible de mutualiser la passerelle Internet sécurisée. Dans ce cas, on parle d'architecture multi-sites (cf. figure 2.19).

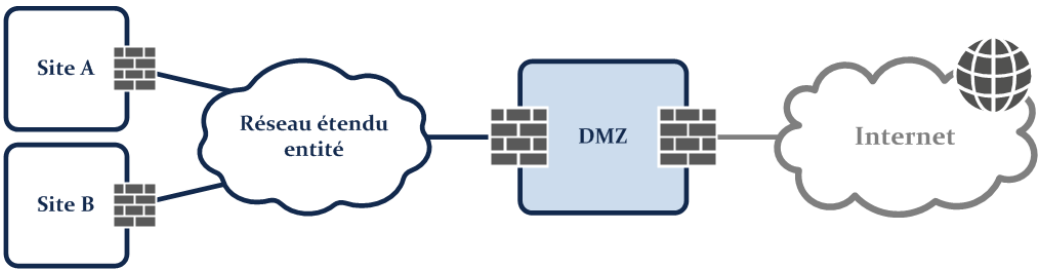


FIGURE 2.19 – Architecture multi-sites

La minimalisation du nombre d'accès à Internet est recommandée dans la mesure où elle simplifie l'exploitation. Toutefois, pour répondre aux besoins de grandes entités (avec de nombreux utilisateurs) ou d'entités disposant de sites géographiques éloignés, il peut être nécessaire, généralement pour des raisons de performance, de démultiplier ce type de passerelle. On parle alors d'architecture multi-zones (cf. figure 2.20).

8. L'acronyme anglais WAN pour *Wide Area Network* est le plus couramment utilisé.

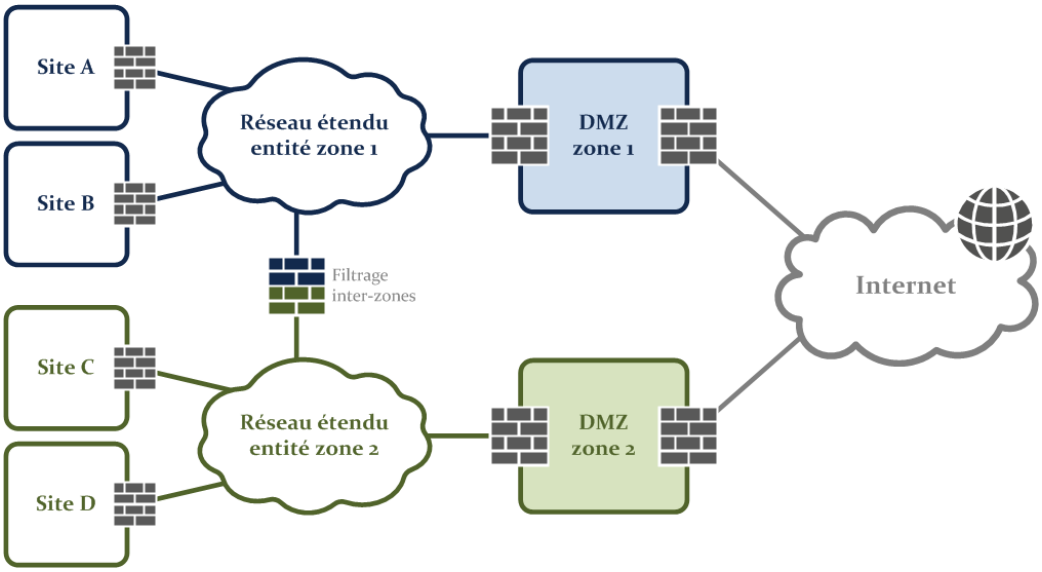


FIGURE 2.20 – Architecture multi-zones

R14

Homogénéiser les passerelles Internet sécurisées dans le cas d'une architecture multi-zones

Dans le cas d'une architecture multi-zones nécessitant de démultiplier le point d'accès à Internet et donc la passerelle Internet sécurisée, il est recommandé de déployer la même architecture (ou un sous-ensemble) et les mêmes produits pour chaque passerelle Internet sécurisée.

Attention

Certaines entités choisissent de mettre en œuvre un service « d'évasion Internet locale ». Cette solution, qui consiste à router le trafic à destination d'Internet vers un accès Internet local au site, est généralement motivée pour des questions de performance en évitant la remontée de trafic Internet jusqu'à une passerelle Internet sécurisée centralisée. Toutefois, du point de vue de la sécurité, elle n'est pas satisfaisante dès que :

- une simple liste de contrôle d'accès (*Access control list*) sur le routeur d'accès est la seule protection périmétrique vis-à-vis d'Internet (non respect de la recommandation R2) ;
- les flux entrants et sortants ne sont pas analysés (non respect de la recommandation R9) ou sont échangés sans protection cryptographique suffisante avec un prestataire externe (cf. recommandation R15).

Toutefois, pour ne pas remettre en cause le concept d'un réseau étendu s'appuyant sur Internet comme réseau de transport, des solutions existent. Par exemple, l'accès Internet local au site peut servir à l'établissement d'un tunnel IPsec et au routage des flux jusqu'à une passerelle Internet sécurisée de l'entité. La conception et la sécurisation d'une telle architecture dépassent le cadre de ce guide.

2.6 Externalisation des fonctions de relais

Pour des raisons opérationnelles ou budgétaires, l'entité peut souhaiter externaliser, généralement grâce à une offre de service logiciel à la demande (SaaS [9]), certaines fonctions de relais (ex : serveur mandataire, antispam…). Si du point de vue de la sécurité, une telle offre peut présenter des avantages de maintien en condition de sécurité et de mise à disposition de fonctions avancées, il est recommandé que cette offre soit qualifiée selon le référentiel d'exigences SecNumCloud [18].

Par ailleurs, dans le cadre d'une analyse de risque, il convient pour l'entité d'identifier les risques spécifiques à l'externalisation d'un de ces services qui sont à considérer comme critiques (cf. le guide afférent de l'ANSSI [2]).

Quoi qu'il en soit, il est nécessaire de protéger en intégrité et en confidentialité l'interconnexion du SI de l'entité avec le fournisseur de service. La mise en place d'un tunnel VPN IPsec est donc recommandée dans ce cas (cf. figure 2.21).

R15

Utiliser une offre qualifiée par l'ANSSI pour les fonctions relais externalisées

Si l'entité fait le choix d'externaliser dans le *cloud* une fonction relais, il est recommandé que le service afférent soit qualifié selon le référentiel d'exigences SecNumCloud [18] de l'ANSSI.
De plus, il est recommandé que l'interconnexion avec le fournisseur du service soit réalisée au travers d'un tunnel VPN IPsec à l'état de l'art (cf. le guide IPSec [7] de l'ANSSI).

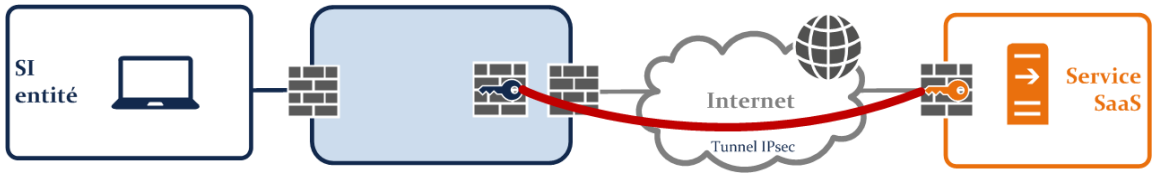


FIGURE 2.21 – Raccordement de la passerelle Internet sécurisée avec un service SaaS assurant une fonction relais

À la date de publication de ce guide, il n'existe pas de telle offre qualifiée par l'ANSSI. Toutefois, pour des entités ayant peu de ressources internes à consacrer à l'exploitation de ces services, il peut être préférable de recourir dès à présent à des services spécialisés externalisés.

R15 -

Évaluer rigoureusement les risques d'une offre non qualifiée par l'ANSSI pour les fonctions relais externalisées

Pour des entités souhaitant externaliser une fonction relais vers une offre de service non qualifiée par l'ANSSI, l'analyse de risque doit être menée avec d'autant plus de rigueur et d'exhaustivité.

9. L'acronyme anglais SaaS pour *Software as a Service* est le plus couramment utilisé.

2.7 Schéma d'architecture multi-services

En conclusion de ce chapitre consacré à l'architecture d'une passerelle Internet sécurisée, il est proposé sur la figure 2.22 un schéma d'architecture multi-services reprenant différents cas d'usage de la passerelle Internet sécurisée qui ne se veulent toutefois pas exhaustifs.

Voici quelques remarques sur les mutualisations et cloisonnements représentés (les numéros de cette liste sont reportés sur la figure 2.22).

Conformément à la recommandation R6 :

1. les pare-feux périmétriques (internes d'une part et externes d'autre part) sont dédiés par chaîne d'usage : flux entrants liés à l'hébergement, flux VPN entrants pour l'accès des collaborateurs au SI, flux sortants ;
2. pour les pare-feux externes, le choix d'un cloisonnement physique (*n* pare-feux physiques dédiés), logique (*n* pare-feux virtuels dédiés sur un socle de pare-feu physique) ou hybride doit être déterminé par l'analyse de risque ; au minimum les pare-feux des chaînes entrantes et sortantes sont physiquement distincts [10] ;
3. la remarque 2 s'applique également pour les pare-feux internes ;
4. s'agissant des ressources (serveurs…) de la zone de services relais, celles-ci sont dédiées par chaîne d'usage et le choix d'un cloisonnement physique (une ressource physique dédiée) ou logique (une machine virtuelle dédiée sur un socle physique mutualisé) doit être déterminé par l'analyse de risque ; au minimum les ressources des chaînes entrantes et sortantes sont physiquement distinctes ;

Par ailleurs :

5. les pare-feux internes et externes ne sont pas mutualisés conformément à la recommandation R13 ;
6. les flux VPN entrants pour l'accès des collaborateurs au SI ne font pas l'objet d'une analyse en amont du concentrateur VPN pour ne pas interrompre le flux IPsec (ou TLS) chiffré et authentifié, conformément au message d'avertissement page 13 ;
7. les flux de synchronisation d'annuaire sont à l'initiative de l'annuaire du SI de l'entité vers l'annuaire dédié de la passerelle Internet sécurisée conformément aux recommandations R7 et R10 ;
8. la passerelle Internet sécurisée est administrée depuis un système d'information d'administration sécurisé, conformément à la recommandation R16 (cf. section 3.1).

10. L'annexe 1 du guide [11] précise les arguments en faveur de l'utilisation de pare-feux physiques.

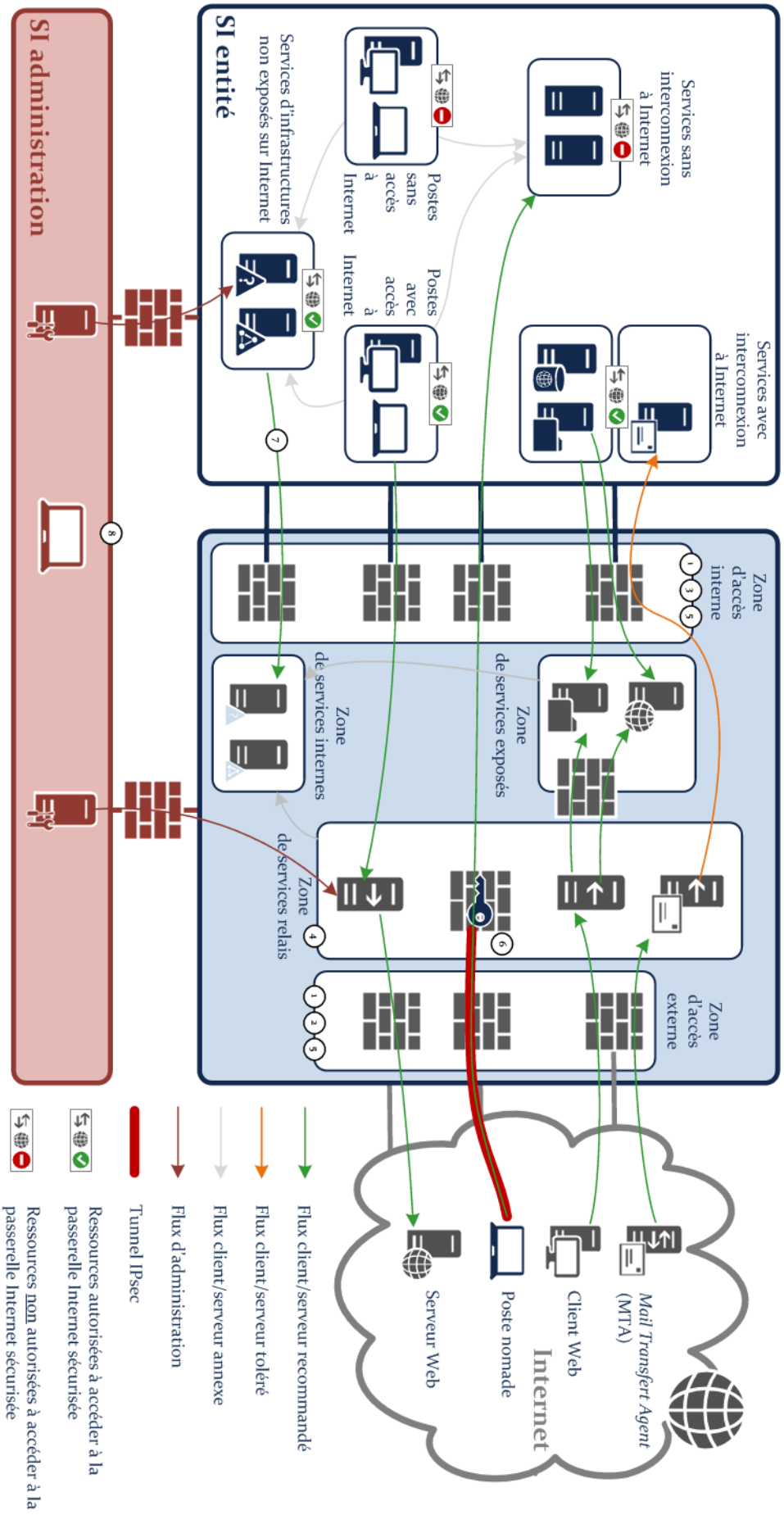


FIGURE 2.22 – Architecture multi-services de la passerelle Internet sécurisée

3
Sécurisation de l'interconnexion

3.1 Administration

Comme toute partie d'un SI, la passerelle Internet sécurisée doit être administrée de manière sécurisée. Pour cela, le lecteur doit se référer aux recommandations de l'ANSSI relatives à l'administration sécurisée.

R16

Administrer de manière sécurisée la passerelle Internet sécurisée

La passerelle Internet sécurisée doit être administrée de manière sécurisée selon les recommandations de l'ANSSI rassemblées dans le guide afférent [12].

3.2 Disponibilité

Comme évoqué en introduction, la disponibilité de l'accès Internet peut être critique pour une entité, qu'il s'agisse des services auxquels elle accède ou des services qu'elle héberge. L'entité doit donc prendre des mesures visant à garantir la disponibilité en phase avec ses objectifs de sécurité.

En premier lieu, il est recommandé de multiplier autant que possible les chemins de raccordement physique (généralement deux) pour éviter tout point unique de rupture.

Par ailleurs, les équipements d'accès (ex : routeurs) peuvent être doublés et/ou double alimentés électriquement pour pallier une panne matérielle ou d'alimentation électrique.

Dans l'hypothèse de deux accès, le choix d'un FAI distinct par accès permet de pallier une interruption de service au niveau d'un cœur de réseau. Dans le cas des accès entrants, cela peut nécessiter un travail de gestion de routage dynamique (gestion d'AS, *Autonomous System*) au niveau de l'interconnexion pour garantir que l'acheminement des flux puisse s'effectuer correctement via l'un ou l'autre des réseaux opérateur.

R17

Garantir la disponibilité attendue grâce à la résilience des accès opérateurs

L'entité doit prendre les mesures nécessaires pour garantir la disponibilité attendue de l'accès à Internet :

- travaux de génie civil pour éviter tout point unique de rupture ;
- déploiement d'équipements supplémentaires pour assurer la redondance matérielle ;
- configuration logicielle pour garantir une résilience réseau protocolaire.

Il est aujourd'hui possible d'acheter en ligne des « prestations » de déni de service distribué (DDoS [11]). Ces prestations sont accessibles pour un coût modique (inférieur à une centaine d'euros) à des profils malveillants ne disposant pas nécessairement de compétences techniques avancées. Ce type d'attaque, s'il réussit, peut nuire fortement à la disponibilité de l'accès Internet de l'entité et donc à son image ou à sa performance. Des solutions techniques, généralement proposées par les FAI, peuvent permettre de contrer une telle attaque.

R18

Mettre en œuvre des contre-mesures aux attaques en déni de service

Qu'il s'agisse d'un service souscrit auprès d'un FAI ou géré en propre par l'entité, il est recommandé de déployer une solution de protection anti-DDoS.

Information

L'ANSSI publie un guide pour comprendre et anticiper les attaques en déni de service distribué [6].

La fonction de routage représente un élément critique de la passerelle Internet sécurisée. En effet, elle détermine l'ensemble des chemins possibles entre le SI de l'entité et Internet. Afin de se prémunir de l'apparition de chemins non souhaités, le routage statique doit être privilégié au sein de la passerelle Internet sécurisée.

R19

Utiliser un routage statique au sein de la passerelle Internet sécurisée

Au sein de la passerelle Internet sécurisée, il est recommandé de déclarer statiquement les routes IP dans les équipements réseau et de désactiver explicitement les protocoles de routage dynamique.

Attention

En particulier, dans le cas d'une éventuelle route par défaut configurée sur le pare-feu interne, il convient de s'assurer que celle-ci n'est pas configurée vers le pare-feu externe (donc vers Internet). En effet, une erreur de configuration avec l'ajout d'une règle de pare-feu interne trop permissive autorisant un flux vers une destination quelconque (*any*) créerait une faiblesse dans l'architecture.
Le cas échéant, il est recommandé de configurer la route par défaut du pare-feu interne vers le SI de l'entité.

3.3 Confidentialité

Afin d'éviter toute fuite d'information sur les politiques de filtrage mises en place vis-à-vis d'Internet, il est recommandé de rendre « silencieux » les pare-feux externes, c'est-à-dire qu'un paquet accepté doit être routé (`ACCEPT`), un paquet refusé doit être ignoré (`DROP`) sans provoquer l'envoi d'une réponse ICMP (`REJECT`).

11. L'acronyme anglais DDoS pour *Distributed Denial of Service* est le plus couramment utilisé.

R20

Ignorer les paquets refusés par la politique des pare-feux externes

Il est recommandé que les connexions refusées par la politique d'un pare-feu externe ne génèrent pas de réponses (mode `DROP` et non `REJECT`).

Afin d'éviter toute fuite d'information technique permettant à un attaquant de reconstituer tout ou partie de l'infrastructure de l'entité, il peut être nécessaire d'anonymiser certains champs techniques (ex : nom et adresse IP des serveurs relais de messagerie dans les en-têtes de courriels, champs *Referer* et *Origin* dans les en-têtes HTTP).

R21

Masquer l'architecture interne vis-à-vis d'Internet

Dès lors que c'est techniquement possible, il est recommandé d'anonymiser les champs techniques divulguant de l'information sur les infrastructures internes de l'entité.

Information

La recommandation R21 est bien à considérer comme complémentaire et moins prioritaire dans la mesure où la sécurité par l'obscurité n'est pas le principe directeur de sécurisation de l'architecture d'interconnexion à Internet.

4
Sécurisation de l'accès aux contenus hébergés sur le Web

L'accès aux contenus hébergés sur le Web (ex : navigation Web des utilisateurs, récupération de sources logicielles pour le maintien en condition de sécurité…) est un des besoins liés à Internet les plus courants pour une entité. Dans ce chapitre, des recommandations spécifiques à la passerelle Internet sécurisée sont d'abord présentées. Des compléments sur la configuration du poste de travail pour la navigation Web des utilisateurs sont ensuite proposés dans la section 4.6 (cf. page 33).

4.1 Mise en place d'un serveur mandataire

Il est essentiel d'éviter tout accès direct depuis un poste utilisateur ou un serveur vers le Web. Pour cela, un serveur mandataire (*proxy*) Web doit assurer le rôle de relais et mettre en œuvre des fonctions de sécurité : authentification, contrôle d'accès, analyse de contenus, journalisation, etc.

On convient de parler d'*un* serveur mandataire mais une grappe (ou *cluster*) de serveurs mandataires peut être déployée pour garantir la haute disponibilité ou séparer des chaînes d'accès (ex : pour les postes de travail d'une part, pour les serveurs d'autre part). À défaut d'être unique, il est recommandé que les serveurs mandataires soient exploités de manière centralisée pour permettre une application simple et rapide des politiques de sécurité et faciliter la journalisation.

R22

Mettre en place un serveur mandataire pour l'accès aux contenus Web

Pour l'accès aux contenus hébergés sur le Web, un serveur mandataire doit être mis en place au sein de la zone de services relais de la passerelle Internet sécurisée.

Pour des raisons opérationnelles ou budgétaires, l'entité peut souhaiter, de manière alternative, souscrire à une offre SaaS de serveur mandataire. Le cas échéant et conformément à R15, il est recommandé que le service soit qualifié selon le référentiel d'exigences SecNumCloud [18] de l'ANSSI et que l'interconnexion avec le fournisseur soit réalisée à travers un tunnel VPN IPsec à l'état de l'art (cf. le guide IPSec [7] de l'ANSSI).

Attention

Il existe sur le marché de nombreuses solutions de serveurs mandataires, libres ou propriétaires. Ce sont généralement des produits complexes, embarquant de nombreuses fonctionnalités. Une bonne maîtrise de cet équipement est alors indispensable pour maîtriser la sécurité de l'accès aux contenus hébergés sur le Web.

Des précisions sur la configuration du serveur mandataire sur les postes de travail sont apportées dans la section 4.6.2 (cf. page 33).

4.2 Authentification

À des fins de contrôle d'accès et d'imputabilité des connexions, il est recommandé d'authentifier tous les accès aux contenus hébergés sur le Web : avec des comptes individuels pour les utilisateurs (exceptionnellement de comptes génériques si le suivi de leur utilisation peut être tracé), des comptes de service pour les applications.

En effet, l'absence d'authentification a plusieurs conséquences :

- il n'est pas possible de réaliser un filtrage spécifique selon les catégories d'utilisateurs (standards, privilégiés, restreints…) ;
- l'accès sortant par un code malveillant s'exécutant sur une ressource interne est facilité ;
- la traçabilité des accès sortants est limitée à l'adresse IP d'origine de la requête (voire celle d'un équipement de routage en cas de traduction d'adresse), et n'intègre pas l'identité de l'utilisateur, ce qui complexifie les recherches en cas d'intrusion.

R23

Authentifier tous les accès aux contenus Web

Tous les accès aux contenus hébergés sur le Web doivent être authentifiés de manière individuelle pour les utilisateurs et non ambiguë pour les services.
À défaut, pour un compte générique, une traçabilité de son utilisation (relevé d'identité) doit être mise en place.

Pour des raisons techniques, il est possible que certains accès ne soient pas authentifiables (ex : logiciel ne prenant pas en charge la saisie d'un identifiant et d'un mot de passe associés à la configuration d'un accès par serveur mandataire). Dans ce cas, une liste blanche peut être gérée sur la base de la source et/ou de la destination (ex : une application hébergée sur un serveur avec une adresse IP fixe interne accédant au site de son éditeur pour réaliser ses mises à jour et ne supportant pas l'authentification). Il est recommandé que le serveur mandataire autorise explicitement les seules adresses IP source à accéder sans authentification au domaine DNS du site de l'éditeur.

R24

Prévoir des restrictions pour les accès non authentifiables

Les exceptions à la recommandation R23 (typiquement les logiciels ne supportant pas l'authentification à un serveur mandataire) doivent être gérées par liste blanche d'adresses IP ou de domaines exemptés d'authentification.
Dans ce cas, il est recommandé d'être le plus proche possible du besoin opérationnel et d'éviter tout ajout à la liste blanche d'un large masque de sous-réseau (ex : supérieur à /24 en IPv4) ou d'un domaine DNS très étendu (ex : `*.moncdn.fr`).

4.3 Interception TLS

Le nombre de sites accessibles en HTTPS est en constante augmentation et constitue une avancée majeure dans la sécurisation des communications dans la mesure où la configuration TLS associée

est à l'état de l'art (cf. le guide TLS de l'ANSSI [9]).

La contrepartie est que, s'il s'agit d'accès à des sites d'hameçonnage (*phishing*) ou d'hébergement de codes malveillants, il est théoriquement impossible de détecter le contenu suspect dans l'ensemble du trafic chiffré. Pour y pallier, la mise en place d'interception TLS est une possibilité. Celle-ci doit permettre *in fine* d'analyser le contenu et de s'assurer de la conformité protocolaire des échanges.

Attention

Tel que mentionné dans le guide de recommandations de sécurité concernant l'analyse des flux HTTPS [8], « *[...] la mise en place de mécanismes de déchiffrement HTTPS présente des risques dans la mesure où cette opération entraîne la rupture d'un canal sécurisé et expose des données en clair au niveau de l'équipement* [12] *en charge de l'opération. Lorsqu'un tel déchiffrement est nécessaire, sa mise en œuvre doit s'accompagner de beaucoup de précautions [...]* ».

L'interception TLS répond donc au besoin de détection de codes malveillants et doit, le cas échéant, être mise en œuvre de façon sécurisée au sein de la zone de services relais. Le choix de l'équipement réalisant cette interception est structurant ; celui-ci doit notamment permettre une configuration des paramètres cryptographiques à l'état de l'art (cf. l'annexe B1 du Référentiel général de sécurité [16]).

R25

Étudier la mise en place d'une interception TLS maîtrisée

Afin de se prémunir de la diffusion de codes malveillants par le biais de sites accessibles en HTTPS, il est recommandé d'étudier la mise en place d'une interception TLS permettant d'analyser le contenu échangé.
Le lecteur doit s'approprier au préalable les recommandations de sécurité concernant l'analyse des flux HTTPS dans le guide [8]. Entre autres, le choix de l'équipement d'interception et la configuration de ses paramètres cryptographiques doivent être considérés avec la plus grande attention.
Enfin, en vertu du respect de la vie privée des collaborateurs, une liste blanche de sites réputés de confiance et non interceptés doit être établie (ex : sites bancaires) et partagée avec les utilisateurs.

Attention

La mise en œuvre d'interception TLS pour détecter des codes malveillants ne se substitue évidemment pas aux mesures de détection propres aux équipements terminaux (ex : antivirus sur les postes de travail ou serveurs accédant au Web).

4.4 Journalisation

Dans le contexte de la passerelle Internet sécurisée et de l'accès aux contenus hébergés sur le Web, il convient de distinguer deux types de journaux :

12. N.D.R. : le serveur mandataire généralement.

- les journaux d'événements techniques des équipements ;
- les journaux d'accès (utilisateurs ou services) aux contenus Web.

Si l'objectif de journalisation peut différer (supervision de sécurité ou investigation numérique *a posteriori* pour les premiers, obligation légale pour les seconds), il convient que ceux-ci soient centralisés et conservés intègres.

R26

Centraliser et sécuriser les journaux liés aux accès Web

L'ensemble des journaux (techniques et fonctionnels) générés par les serveurs mandataires doivent être centralisés, de préférence par l'intermédiaire d'un réseau d'administration dédié (cf. R16).
Il est recommandé de consulter les recommandations de sécurité de l'ANSSI pour la mise en œuvre d'un système de journalisation [4], en particulier le paragraphe C.3.1 sur la conservation des éléments de journalisation par les fournisseurs d'accès à Internet.

4.5 Déploiement de postes de rebond

Pour les entités ayant des objectifs élevés de sécurité, il peut être envisagé de déployer une infrastructure de postes de rebond sur lesquels les utilisateurs se connectent depuis leur poste bureautique par accès à distance. *In fine* ce sont les postes de rebond qui permettent de naviguer sur le Web. La rupture protocolaire permise par l'accès à distance renforce le cloisonnement du poste bureautique vis-à-vis d'Internet. De façon complémentaire, ces postes de rebond peuvent être des machines virtuelles temporaires, détruites après utilisation afin d'éviter toute persistance d'une attaque.

Même dans ce cas de figure et conformément à R22, les postes de rebond accèdent aux contenus Web à travers un serveur mandataire. De plus, il sont dédiés à cet usage et ne permettent pas d'autres utilisations (ex : pas d'autres applications installées qu'un navigateur Web). Cette architecture est représentée sur la figure 4.1.

R27 *

Déployer des postes de rebond pour la navigation Web

Pour répondre à des objectifs de sécurité élevés, il est recommandé de déployer une infrastructure de postes de rebond dédiés à la navigation Web sur lesquels les utilisateurs se connectent par accès à distance depuis leur poste de travail bureautique.
Les postes de rebond doivent utiliser le serveur mandataire de la passerelle Internet sécurisée pour accéder aux contenus hébergés sur le Web.

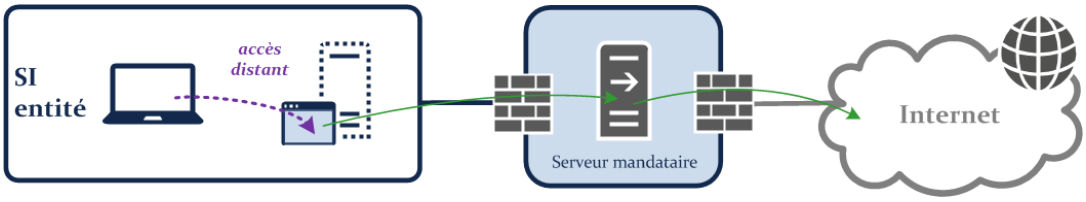


FIGURE 4.1 – Infrastructure de postes de rebond pour la navigation Web

4.6 Configuration des postes de travail pour la navigation Web

Avant tout, les postes de travail des utilisateurs sont supposés conformes aux pratiques d'hygiène informatique, dont entre autres :

- être à jour (système d'exploitation et logiciels) ;
- activer un pare-feu local ;
- disposer d'un anti-virus.

4.6.1 Maîtrise d'un ou plusieurs navigateurs Web

L'ANSSI ne se prononce pas en faveur de tel ou tel navigateur Web : Microsoft Internet Explorer ou Edge, Google Chrome, Mozilla Firefox… Chacun présente ses avantages et inconvénients fonctionnels et de sécurité.

L'utilisation d'un navigateur Web conforme aux standards du Web et maintenu à jour par son éditeur est indispensable. La maîtrise de son déploiement et de son exploitation (configuration centralisée, mises à jour, gestion des greffons ou *plugins*…) constitue dès lors l'enjeu majeur du point de vue de la sécurité. Le déploiement maîtrisé d'une seule solution est préférable par rapport au déploiement de plusieurs solutions inégalement maîtrisées.

R28

Maîtriser le déploiement et l'exploitation du ou des navigateurs Web

En tant qu'interface d'accès des utilisateurs au Web, le ou les navigateurs Web déployés sur les postes de travail doivent être configurés et mis à jour selon des procédures strictes.
En particulier leur surface d'attaque doit être réduite au strict nécessaire par désactivation de tout module ou paramètre inutile.

Certaines entités font le choix de déployer un navigateur pour la navigation interne (ex : sites intranet) et un navigateur pour la navigation Web. Cette solution peut constituer une bonne pratique dans la mesure où la recommandation R28 est respectée pour les deux navigateurs. En effet, si l'entité doit maintenir un navigateur interne obsolète pour des raisons fonctionnelles (ex : une application métier historique non conforme aux standards Web), il n'est pas suffisant de considérer qu'il est « moins exposé » ; des mesures complémentaires doivent être prises, par exemple la conteneurisation du navigateur voire l'utilisation de postes de travail dédiés.

4.6.2 Configuration du serveur mandataire

Pour une meilleure maîtrise des flux sur le réseau de l'entité, le serveur mandataire doit être configuré en mode *explicite* et non *transparent* vis-à-vis des clients. Cela se justifie par deux raisons :

- éviter un routage d'adresses IP publiques sur le réseau privé de l'entité, voire un routage par défaut vers ce serveur mandataire – un serveur mandataire configuré en mode transparent sur les clients doit « attirer » le trafic à destination d'Internet ;

- pouvoir interdire les résolutions DNS publiques (ex : adresse Web) depuis les postes de travail ; celles-ci sont alors inutiles localement car gérées par le serveur mandataire et le risque d'une exfiltration par le canal DNS depuis le poste est ainsi réduit (cf. paragraphe 2.4.6 page 20).

R29

Configurer le serveur mandataire en mode explicite

Du point de vue de la sécurité, le serveur mandataire doit être configuré en mode explicite sur les clients.

Afin de ne pas affaiblir le niveau global de sécurité du SI de l'entité, il est nécessaire que tous les postes de travail, y compris les postes nomades, ne puissent pas accéder directement à Internet. En situation de nomadisme, il est fortement recommandé que les postes de travail se connectent de manière sécurisée à travers un tunnel VPN au SI de l'entité puis accèdent à Internet à travers la passerelle Internet sécurisée (cf. figure 3.2 du guide de l'ANSSI sur le nomadisme numérique [13]).

R30

Empêcher le contournement du serveur mandataire

Il doit être techniquement impossible pour l'utilisateur de contourner les équipements de sécurité pour accéder à Internet.
En particulier, la configuration du serveur mandataire dans les navigateurs Web doit être non modifiable par l'utilisateur ou un logiciel tiers.
Dans un souci de défense en profondeur, le pare-feu local des postes de travail doit bloquer tout accès direct à Internet (sauf exception pour l'accès au concentrateur VPN de l'entité).
Cette recommandation est également valable pour toute autre ressource (ex : serveur ou mobile multifonction [13] sous contrôle de l'entité) nécessitant d'accéder au Web à travers un navigateur ou les protocoles HTTP/HTTPS.

Attention

Si cette configuration est incompatible avec les technologies de portail captif, elle est le seul moyen de garantir que le poste sera protégé en toutes circonstances. Même temporaire, un accès à ce type de portail annihile la confiance dans un poste. L'utilisation de solutions d'accès alternatives est recommandée.

Le serveur mandataire peut être déclaré simplement par une politique de configuration (ex : *Group Policy Object* sur Windows) permettant l'ajout d'un nom DNS ou d'une adresse IP dans les paramètres du navigateur Web.

R31

Appliquer une politique de configuration locale du serveur mandataire

Il est recommandé de déclarer le serveur mandataire localement sur les postes accédant à Internet, idéalement grâce à une politique de configuration.
Cette recommandation est également valable pour toute autre ressource (ex : serveur ou mobile multifonction [13] sous contrôle de l'entité) nécessitant d'accéder au Web à travers un navigateur ou les protocoles HTTP/HTTPS.

13. Le terme anglais *smartphone* est plus couramment utilisé.

En complément, des plages d'adresses IP (ex : plage privée 10.0.0.0/8) ou des noms de domaine locaux peuvent être déclarés en exception pour éviter l'envoi de trafic interne au SI de l'entité vers le serveur mandataire de la passerelle Internet sécurisée.

Information

Supporté par la plupart des navigateurs, le fichier .PAC (*proxy auto-config*) permet de définir finement la politique de configuration du serveur mandataire, en fonction de la destination notamment. Par exemple, les flux internes sont envoyés directement alors que les flux à destination d'Internet sont envoyés vers le serveur mandataire.
Un déploiement du fichier .PAC directement sur les postes de travail est possible. Toutefois, la mise à disposition sur un serveur Web interne est généralement préférée. En effet, cela permet une reconfiguration plus rapide au besoin, sans nécessité de redéployer le fichier unitairement par poste.
Le cas échéant, l'adresse cible du fichier PAC (ex : `https://monserveur/proxy.pac`) est spécifiée dans la configuration des navigateurs. Ce fichier doit être récupéré via le protocole HTTPS et non HTTP. Le certificat du serveur Web doit être signé par une autorité de certification déclarée au niveau du navigateur.
Cette solution alternative à la recommandation R31 présente des avantages fonctionnels mais induit un risque d'interception et d'altération du fichier de configuration pouvant mener à un détournement du trafic.

Attention

Le protocole *Web Proxy Autodiscovery Protocol* (WPAD) est une alternative au fichier .PAC ; il s'appuie sur DHCP et DNS pour la récupération d'un fichier de configuration `wpad.dat`. Même s'il est relativement simple à mettre en œuvre pour le déploiement d'une configuration automatique de serveur mandataire, plusieurs vulnérabilités affectent ce protocole. Son utilisation est donc à proscrire *absolument*.

Liste des recommandations

Bibliographie

[1] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://www.ssi.gouv.fr/nt-commutateurs.

[2] *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information*.
Guide Version 1.0, ANSSI, décembre 2010.
https://www.ssi.gouv.fr/infogerance.

[3] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://www.ssi.gouv.fr/hygiene-informatique.

[4] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[5] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://www.ssi.gouv.fr/politique-filtrage-parefeu.

[6] *Comprendre et anticiper les attaques DDoS*.
Guide Version 1.0, ANSSI, mars 2015.
https://www.ssi.gouv.fr/guide-ddos.

[7] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[8] *Recommandations de securité concernant l'analyse des flux HTTPS*.
Note technique DAT-NT-019/ANSSI/SDE/NP v1.2, ANSSI, février 2016.
https://www.ssi.gouv.fr/analyse-https.

[9] *Recommandations de sécurité relatives à TLS*.
Guide SDE-NT-035 v1.1, ANSSI, août 2016.
https://www.ssi.gouv.fr/nt-tls.

[10] *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.
https://www.ssi.gouv.fr/nettoyage-politique-fw.

[11] *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet*.
Guide ANSSI-PA-044 v1.0, ANSSI, janvier 2018.
https://www.ssi.gouv.fr/guide-pare-feux-internet.

[12] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[13] *Recommandations sur le nomadisme numérique*.
Guide ANSSI-PA-054 v1.0, ANSSI, octobre 2018.
https://ssi.gouv.fr/nomadisme-numerique.

[14] *Définition d'une architecture de passerelle d'interconnexion sécurisée*.
Guide Version 1.0, ANSSI, décembre 2011.
https://www.ssi.gouv.fr/architecture-interconnexion.

[15] *Instruction générale interministérielle n°1300*.
Référentiel Version 1.0, ANSSI, novembre 2011.
https://www.ssi.gouv.fr/igi1300.

[16] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[17] *Instruction interministérielle n°901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://www.ssi.gouv.fr/ii901.

[18] *Prestataires de services d'informatique en nuage (SecNumCloud). Référentiel d'exigences*.
Référentiel 3.1, ANSSI, juin 2018.
https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf.

[19] *Licence ouverte / Open Licence*.
Page Web v2.0, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

ANSSI-PA-066
Version 2.0 - 18/06/2019

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Le Ministre

Paris, le 26 MAR 2015

Le ministre de l'intérieur

à

Monsieur le préfet de police
Mesdames et Messieurs les préfets de département
Monsieur le préfet de police des Bouches-du-Rhône

Copie pour information à
Monsieur le directeur général de la police nationale
Monsieur le directeur général de la gendarmerie nationale

CIRCULAIRE NOR : INTD1502555C

OBJET : Procédure de la levée de doute des télésurveilleurs

REF : Article L.613-6 du code de la sécurité intérieure

Résumé : Cette circulaire a pour objet de clarifier la procédure de la levée de doute imposée par la loi aux entreprises de télésurveillance afin de limiter, d'une part, les interventions injustifiées des forces de police ou de gendarmerie et, d'autre part, les risques de sanctions pécuniaires auxquels s'exposent les entreprises concernées. Vous pouvez utilement présenter cette méthodologie aux forces de police et de gendarmerie placées sous votre autorité.

L'article L.613-6 du code de la sécurité intérieure dispose que :

« *Est injustifié tout appel des services de la police nationale ou de la gendarmerie nationale par les personnes physiques ou morales exerçant des activités de surveillance à distance des biens meubles ou immeubles qui entraîne l'intervention indue de ces services, faute d'avoir été précédé d'une levée de doute consistant en un ensemble de vérifications, par ces personnes physiques ou morales, de la matérialité et de la concordance des indices laissant présumer la commission d'un crime ou délit flagrant concernant les biens meubles ou immeubles. L'autorité administrative peut prononcer à l'encontre des personnes physiques ou morales mentionnées à l'alinéa précédent qui appellent sans justification les services de la police nationale ou de la gendarmerie nationale une sanction pécuniaire d'un montant qui ne peut excéder 450 euros par appel injustifié.*

L'autorité administrative peut prononcer à l'encontre des personnes physiques ou morales mentionnées à l'alinéa précédent qui appellent sans justification les services de la police nationale ou de la gendarmerie nationale une sanction pécuniaire d'un montant qui ne peut excéder 450 euros par appel injustifié.

La personne physique ou morale à l'encontre de laquelle est envisagée la sanction pécuniaire prévue au précédent alinéa est mise en mesure de présenter ses observations avant le prononcé de la sanction et d'établir la réalité des vérifications qu'elle a effectuées, mentionnées au premier alinéa.

Cette sanction pécuniaire est recouvrée comme les créances de l'Etat étrangères à l'impôt et au domaine. Elle est susceptible d'un recours de pleine juridiction. »

La définition de la levée de doute consiste ainsi en un ensemble de vérifications, par les personnes physiques ou morales, de la matérialité et de la concordance des indices laissant présumer la commission d'un crime ou délit flagrant concernant les biens meubles ou immeubles.

Cette définition indique bien que la levée de doute est obligatoire dans le cadre de la commission d'un crime ou délit flagrant concernant les biens meubles et immeubles. Ainsi, dans le cas d'un crime ou d'un délit flagrant d'atteinte aux personnes, le texte ne prévoit pas une levée de doute effectuée par les télésurveilleurs.

Le fondement juridique de l'intervention des services de police et de gendarmerie est la procédure de flagrant délit puisque leur action se situe dans l'hypothèse d'un « crime ou d'un délit qui se commet actuellement ou qui vient de se commettre » prévue aux articles 53 et suivants du code de procédure pénale. Cette intervention correspond à une opération de police judiciaire.

Il est donc nécessaire que des indices apparents d'un comportement délictueux révélant une infraction répondant à la définition des crimes et délits flagrants existent préalablement à l'entrée des officiers et agents de police judiciaire dans les lieux surveillés à distance.

En raison de l'extrême sensibilité des détecteurs utilisés pour les systèmes d'alarmes « passifs » (détecteurs volumétriques, thermiques, capteurs de pression) engendrant de nombreux déclenchements intempestifs, la levée de doute pourrait répondre à la procédure suivante :

- en présence d'images non équivoques, confortées par l'existence d'éléments permettant de confirmer leur caractère inhabituel (liste des horaires de présence du personnel habilité, zones de passage autorisé, etc.) la réalité de l'atteinte aux personnes ou aux biens et immeubles est avérée et la levée de doute est réputée effectuée (CAA Versailles, 2014, n°13VE02603).

- en l'absence d'images non équivoques, une prise de contact avec le client est indispensable. Si le client est une entreprise, deux appels successifs peuvent être effectués auprès du ou des responsables déclarés afin de vérifier la situation. S'il s'agit d'un particulier, deux appels peuvent être réalisés dans les mêmes conditions auprès des personnes désignées par le contrat de prestation. Au terme de ces deux appels :

    - si la prise de contact avec le client a lieu, et se révèle fructueuse, la levée de doute est effectuée.

- si les tentatives de prise de contact avec le client se soldent par un échec, ou si un doute subsiste sur la commission d'un crime ou d'un délit flagrant concernant les biens meubles ou immeubles, il appartient à l'entreprise de télésurveillance de réaliser une vérification effective des causes du déclenchement des détecteurs par au moins deux éléments parmi les suivants : images vidéo, écoute des sons pouvant être émis dans le lieu surveillé, interaction phonique, concordance entre différentes alarmes, **ou,** en l'absence d'éléments concordants apparaissant à l'usage de ces procédés, par l'envoi d'un agent sur place. La levée de doute est alors réputée effectuée.

A votre initiative, pour répondre aux exigences des politiques de sécurité publique et raccourcir les délais d'intervention des forces de police et de gendarmerie, la procédure de levée de doute à mettre en œuvre peut être définie, localement, d'un commun accord entre les forces de l'ordre et les entreprises de télésurveillance pour des périodes et des lieux précis.

Par exemple, dans une zone délimitée, dans le cadre de la lutte contre les vols avec effraction, sur une période critique à préciser, il peut être convenu que les forces de sécurité intérieure seront sollicitées dès le déclenchement de l'alarme sur un site défini comme sensible (bijouterie, banque, entreprise de stockage de métaux, grande surface, etc.).

Enfin, dans la mesure où le délai de conservation des données images par les opérateurs de télésurveillance a été fixé à un mois maximum par l'article L.252-5 du code de la sécurité intérieure, il est recommandé aux services de la police et de la gendarmerie nationales de solliciter la transmission des données qui leur seraient nécessaires dans ce délai.

Vous veillerez à la diffusion de cette pratique, qui permettra de faciliter et de mieux définir les échanges entre les forces de sécurité intérieure et les entreprises chargées de la surveillance par des dispositifs électroniques.

Vous me rendrez compte, sous le timbre de la direction des libertés publiques et des affaires juridiques et de la délégation aux coopérations de sécurité, de toute difficulté rencontrée dans la mise en œuvre de cette circulaire.

Bernard CAZENEUVE

PREFECTURE DES HAUTS-DE-SEINE

DIRECTION REGIONALE ET INTERDEPARTEMENTALE
DE L'EQUIPEMENT ET DE L'AMENAGEMENT
D'ILE-DE-FRANCE
Unité territoriale des Hauts-de-Seine

DIRECTION REGIONALE ET INTERDEPARTEMENTALE
DE L'ENVIRONNEMENT ET DE L'ENERGIE
D'ILE-DE-FRANCE
Unité territoriale des Hauts-de-Seine

Commune de GENNEVILLIERS (92)

Plan de Prévention des Risques Technologiques

Dépôts pétroliers de la

Société de Gestion des Produits Pétroliers
Société des Transports Pétroliers par Pipeline

Approuvé par arrêté préfectoral n° 2012-234

✗ Note de présentation

✗ Plan de zonage réglementaire

✗ **Règlement**

✗ Cahier des recommandations

Vu pour être annexé à l'arrêté préfectoral n° 2012-234 du 21 décembre 2012 portant approbation du plan de prévention des risques technologiques des dépôts pétroliers classés « AS » exploités par les sociétés SOGEPP et TRAPIL et situés à Gennevilliers

Pierre-André REYVEL

Table des matières

Titre I - Dispositions générales

Ce Plan de Prévention des Risques Technologiques (PPRT) a pour objet de limiter les effets d'accidents susceptibles de survenir dans les installations des dépôts pétroliers de la Société de Gestion des Produits Pétroliers (SOGEPP) et de la société des Transports Pétroliers par Pipeline (TRAPIL), et pouvant entraîner des effets sur la salubrité, la santé et la sécurité publiques conformément à l'article L.515-15 du code de l'environnement.

Pour répondre à l'objectif de sécurité de la population, le PPRT permet d'agir :

- d'une part, sur la réduction de la situation de vulnérabilité des personnes déjà implantées à proximité des sites industriels, en agissant en particulier sur le bâti existant et en mettant en œuvre des mesures foncières si nécessaire ;
- d'autre part, sur la maîtrise du développement de l'urbanisation future, avec notamment des prescriptions et/ou des recommandations sur le bâti futur.

I.1 - Champ d'application

Le présent règlement du PPRT lié aux dépôts pétroliers des sociétés SOGEPP et TRAPIL, implantés sur la commune de Gennevilliers, s'applique aux différentes zones situées sur le territoire de la commune de Gennevilliers (92) à l'intérieur du périmètre d'exposition aux risques, cartographiées sur le plan de zonage réglementaire joint.

I.2 - Effets du règlement

En application des articles L.515-15 et suivants du code de l'environnement, le présent règlement délimite, à l'intérieur du périmètre d'exposition aux risques, plusieurs types de zones. Sept zones, de réglementation différente, ont été définies en fonction du type de risques, de leur gravité, de leur probabilité, de leur cinétique et des enjeux en présence :


Zone R


Zone r


Zone B1


Zone B2

Zone b1

Zone b2

Zone G

Les critères et la méthodologie ayant présidé à la détermination de ces zones sont exposés dans la note de présentation jointe.

Un projet empiétant sur deux zones réglementées se verra appliquer les principes réglementaires de la zone la plus contraignante.

Dans ces zones, la réalisation d'aménagements ou d'ouvrages ainsi que les constructions nouvelles et l'extension de constructions existantes peuvent être interdites ou subordonnées au respect de prescriptions relatives à la construction, à l'utilisation ou à l'exploitation.

Des mesures de protection des populations face aux risques encourus, relatives à l'aménagement, l'utilisation ou l'exploitation des constructions, des ouvrages, des installations et des voies de communication peuvent également être prescrites dans ces zones.

La commune ou l'établissement public de coopération intercommunale compétent peut instaurer le droit de préemption urbain sur l'ensemble du périmètre d'exposition aux risques, dans les conditions définies aux articles L.211-1 et suivants du code de l'urbanisme.

Aucun secteur défini à l'article L.515-16 du code de l'environnement n'a été ouvert aux mesures d'expropriation ou de délaissement.

Le PPRT comporte également des recommandations explicitées dans le cahier de recommandations auquel il convient de se reporter pour connaître les dispositions préconisées :

- dans les zones réglementées, où certaines recommandations peuvent venir compléter les mesures de protection des populations prescrites au titre IV notamment lorsque ces dernières dépassent 10% de la valeur vénal des biens ;
- dans les zones règlementées, pour les biens exposés à plusieurs effets, lorsque pour l'un d'entre eux, le niveau d'aléa n'engendre pas de prescription.

La zone hors du périmètre d'exposition aux risques n'est pas directement exposée aux aléas. Aucune occupation ou utilisation du sol n'y est interdite ni même restreinte, au titre du présent PPRT.

I.3 - Application et mise en œuvre du PPRT

Le présent PPRT approuvé vaut servitude d'utilité publique conformément à l'article L.515-23 du code de l'environnement.

Il est porté à la connaissance du maire de la commune située dans le périmètre d'exposition aux risques en application de l'article L.121-2 du code de l'urbanisme et, conformément à l'article L.126-1 du code de l'urbanisme, annexé au plan local d'urbanisme dans un **délai de 3 mois** à compter de la date de sa réception selon la procédure de mise à jour prévue à l'article R.123-22 du code de l'urbanisme.

Les constructions, installations, travaux ou activités non soumis à un régime de déclaration ou d'autorisation préalable sont édifiés ou entrepris sous la seule responsabilité de leurs auteurs.

La mise en œuvre des prescriptions édictées par le PPRT relève de la responsabilité des maîtres d'ouvrage pour les projets futurs, et des propriétaires, exploitants et utilisateurs, dans les délais que le plan détermine, pour l'existant.

Les infractions aux prescriptions du PPRT sont punies des peines prévues à l'article L.480-4 du code de l'urbanisme.

Le PPRT peut être révisé dans les conditions prévues par l'article R.515-47 du code de l'environnement, sur la base d'une évolution de la connaissance ou du contexte.

Titre II - Réglementation des zones

On entend par « **projet** » les éléments définis ci-dessous et **soumis à une formalité au titre du code de l'urbanisme** :

- les constructions, les extensions et les annexes des constructions existantes ainsi que l'aménagement de leur terrain ;
- les réalisations et les extensions d'infrastructures de transport ;
- les réalisations d'ouvrages et d'équipements techniques ;
- les travaux sur les constructions, infrastructures, ouvrages et équipements techniques existants ;
- les réalisations d'aménagements d'espace public de proximité : de camping, d'aires d'accueil des gens du voyage et de parkings ;
- les démolitions ;
- les reconstructions en cas de sinistre lié à l'aléa technologique ;
- les changements de destination ;

Le présent PPRT réglemente les projets dont les demandes d'autorisation et les déclarations sont déposées après la date d'approbation du PPRT.

On entend par « **activité** », toutes les activités économiques recensées par la nomenclature des activités économiques (NAF version 2 de 2008) définie par l'INSEE, à l'exception des établissements recevant du public.

On entend par « **activité sans présence humaine permanente** », les activités ne nécessitant pas la présence de personnel pour fonctionner. Celle-ci est liée uniquement à l'intervention pour des opérations ponctuelles (opérations de maintenance par exemple).

On entend par « **activité à faible enjeu** », les activités au sein desquelles les salariés ne sont pas présents de façon permanente, c'est-à-dire qu'ils exercent leurs tâches à l'extérieur du site de façon majoritaire. Ce critère est défini sur la base du principe suivant : tous les salariés à l'extérieur de la zone pendant une part très significative de leur temps de travail supérieure à 90%.

On entend par « **bien** », toutes propriétés mobilières ou immobilières.

On entend par « **Établissement Recevant du Public (ERP)** », tous bâtiments, locaux et enceintes définis par l'article R.123-2 du code de la construction et de l'habitation.

On entend par « **Établissement Recevant du Public difficilement évacuable** », les ERP pour lesquels, compte-tenu de la durée de développement des phénomènes dangereux considérés, les occupants ne disposent pas du temps suffisant pour évacuer le bâtiment et quitter la zone des effets considérés (établissements scolaires, de soins, ceux accueillant des personnes à mobilité réduite comme les maisons de retraite, prison, grandes surfaces commerciales…).

On entend par « **infrastructure** » l'ensemble de la plateforme (ainsi que son traitement paysager) qu'il est nécessaire d'aménager pour permettre le fonctionnement des systèmes de transports routiers, ferrés, fluviaux et doux.

II.1 - Dispositions applicables en zone R

On rappelle que les termes utilisés dans le paragraphe II.1 sont définis au titre II page 6.

II.1.1 - Dispositions applicables aux projets nouveaux

Article 1 - Projets nouveaux interdits

Hormis les projets autorisés à l'article 2, tous les projets nouveaux sont interdits.

Article 2 - Projets nouveaux autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.1.3 :

- les constructions à usage d'activité industrielle et les aménagements de leur terrain, directement en lien avec l'activité à l'origine du risque sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité et de ne pas accueillir de public ;

- les constructions, à usage d'activité participant au service portuaire et les aménagements de leur terrain, limitées :
  - ✗ aux activités de chargement / déchargement ;
  - ✗ aux activités de manutention sur les aires ou entrepôts de transit ou de stockage de marchandises directement liées aux installations de chargement / déchargement ;
  - ✗ aux activités de transformation des matériaux ;

  sous réserve de constituer une activité à faible enjeu et de ne pas accueillir de public ;

- les constructions à usage d'activité à faible enjeu ;

- la réalisation d'ouvrages de protection :
  - ✗ des constructions ;
  - ✗ des infrastructures ;
  - ✗ des équipements techniques.

Sont également admis :

- les équipements techniques de services publics (ouvrages de distribution d'énergie, de produits pétroliers, d'alimentation d'eau potable, d'assainissement, de télécommunication...) sous réserve de ne pas générer de présence humaine permanente ;

- la réalisation d'infrastructures strictement nécessaires aux secours ou aux activités à proximité immédiate de la zone R ou au fonctionnement des services d'intérêt général.

II.1.2 - Dispositions applicables aux projets sur les biens et activités existants

Article 3 - Projets sur les biens et activités existants interdits

Hormis les projets autorisés à l'article 4, tous les projets sur les biens et activités existants sont interdits.

Zone R

Article 4 - Projets sur les biens et activités existants autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.1.3 :

- les extensions et les travaux sur les constructions à usage d'activité et les aménagements de leur terrain sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité ;
- les extensions et les travaux sur les constructions à usage d'activité à faible enjeu ainsi que l'aménagement de leur terrain, sous réserve de ne pas générer de présence humaine permanente ;
- les travaux nécessaires au changement de destination de constructions existantes à usage d'activité à faible enjeu sous réserve de ne pas générer de présence humaine permanente ;
- les travaux sur les ouvrages de protection.

Sont également admis :

- les extensions et les travaux sur les équipements techniques et les aménagements de leur terrain sous réserve de ne pas générer de présence humaine permanente ;
- les travaux sur les infrastructures ;
- les changements de destination à usage d'activité à faible enjeu sans présence humaine permanente ;
- les démolitions ;
- les travaux d'entretien des chemins de halage ;
- les travaux d'entretien et de stabilisation des berges des darses ;
- les travaux des espaces libres (plantations, dépollution, clôtures...) sous réserve de ne pas les ouvrir au public et de ne pas générer de présence humaine permanente.

II.1.3 - Prescriptions constructives

Les projets doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets de surpression et des effets thermiques continus et transitoires dont l'intensité est donnée en annexe du présent règlement.

Ces caractéristiques sont définies par une étude préalable[1] à la charge du maître d'ouvrage.

Font exceptions à cette obligation les extensions de bâtiments d'activité dont la surface de plancher est inférieure à 40 m² et ne nécessitant pas une présence humaine permanente.

1 Conformément à l'article *R.431.16.c) du code de l'urbanisme, la demande de permis de construire comporte une attestation certifiant la réalisation de cette étude et constatant que le projet prend en compte ces conditions au stade de la conception.

II.2 - Dispositions applicables en zone r

On rappelle que les termes utilisés dans le paragraphe II.2 sont définis au titre II page 6.

II.2.1 - Dispositions applicables aux projets nouveaux

Article 5 - Projets nouveaux interdits

Hormis les projets autorisés à l'article 6, tous les projets nouveaux sont interdits.

Article 6 - Projets nouveaux autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.2.3 :

- les constructions à usage d'activité industrielle et les aménagements de leur terrain, directement en lien avec l'activité à l'origine du risque sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité et de ne pas accueillir de public ;

- les constructions à usage d'activité participant au service portuaire et les aménagements de leur terrain, limitées :
  - ✗ aux activités de chargement / déchargement ;
  - ✗ aux activités de manutention sur les aires ou entrepôts de transit ou de stockage de marchandises directement liées aux installations de chargement / déchargement ;
  - ✗ aux activités de transformation des matériaux ;

  sous réserve de constituer une activité à faible enjeu et de ne pas accueillir de public ;

- les constructions à usage d'activité à faible enjeu ;

- la réalisation d'ouvrages de protection :
  - ✗ des constructions ;
  - ✗ des infrastructures ;
  - ✗ des équipements techniques.

Sont également admis :

- les équipements techniques de services publics (ouvrages de distribution d'énergie, de produits pétroliers, d'alimentation d'eau potable, d'assainissement, de télécommunication...) sous réserve de ne pas générer de présence humaine permanente ;

- la réalisation d'infrastructures strictement nécessaires aux secours ou aux activités à proximité immédiate de la zone r ou au fonctionnement des services d'intérêt général.

II.2.2 - Dispositions applicables aux projets sur les biens et activités existants

Article 7 - Projets sur les biens et activités existants interdits

Hormis les projets autorisés à l'article 4, tous les projets sur les biens et activités existants sont interdits.

Article 8 - Projets sur les biens et activités existants autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.2.3 :

- les extensions et les travaux sur les constructions à usage d'activité et les aménagements de leur terrain sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité ;
- les extensions et les travaux sur les constructions à usage d'activité à faible enjeu ainsi que l'aménagement de leur terrain, sous réserve de ne pas générer de présence humaine permanente ;
- les travaux nécessaires au changement de destination de constructions existantes à usage d'activité à faible enjeu sous réserve de ne pas générer de présence humaine permanente ;
- les reconstructions en cas de sinistre, sans changement de destination ;
- les travaux sur les ouvrages de protection.

Sont également admis :

- les travaux sur les équipements techniques et les aménagements de leur terrain sous réserve de ne pas générer de présence humaine permanente ;
- les travaux sur les infrastructures ;
- les changements de destination à usage d'activité à faible enjeu sans présence humaine permanente ;
- les démolitions ;
- les travaux d'entretien des chemins de halage ;
- les travaux d'entretien et de stabilisation des berges des darses ;
- les travaux des espaces libres (plantations, dépollution, clôtures...) sous réserve de ne pas les ouvrir au public et de ne pas générer de présence humaine permanente.

II.2.3 - Prescriptions constructives

Les projets doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des des effets thermiques continus et transitoires dont l'intensité est donnée en annexe du présent règlement.

Ces caractéristiques sont définies par une étude préalable[2] à la charge du maître d'ouvrage.

Font exceptions à cette obligation les extensions de bâtiments d'activité dont la surface de plancher est inférieure à 40 m² et ne nécessitant pas une présence humaine permanente.

2 Conformément à l'article *R.431.16.c) du code de l'urbanisme, la demande de permis de construire comporte une attestation certifiant la réalisation de cette étude et constatant que le projet prend en compte ces conditions au stade de la conception.

II.3 - Dispositions applicables en zones B1 et B2

On rappelle que les termes utilisés dans le paragraphe II.3 sont définis au titre II page 6.

II.3.1 - Dispositions applicables aux projets nouveaux

Article 9 - Projets nouveaux interdits

Hormis les projets autorisés à l'article 10, tous les projets nouveaux sont interdits.

Article 10 - Projets nouveaux autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.3.3 :

- les constructions à usage d'activité et les aménagements de leur terrain sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité et de ne pas accueillir de public ;

- la réalisation d'ouvrages de protection :
  - ✗ des constructions ;
  - ✗ des infrastructures ;
  - ✗ des équipements techniques.

Sont également admis :

- les constructions d'équipements techniques de services publics (ouvrages de distribution d'énergie, de produits pétroliers, d'alimentation d'eau potable, d'assainissement, de télécommunication...) sous réserve de ne pas générer de présence humaine permanente ;
- la réalisation d'infrastructures strictement nécessaires aux secours ou aux activités à proximité immédiate des zones B1 et B2 ou au fonctionnement des services d'intérêt général ;
- les aires de stationnement liées aux activités autorisées et celles nécessaires aux services publics ou d'intérêts collectifs.

II.3.2 - Dispositions applicables aux projets sur les biens et activités existants

Article 11 - Projets sur les biens et activités existants interdits

Hormis les projets autorisés à l'article 12, tous les projets sur les biens et activités existants sont interdits.

Article 12 - Projets sur les biens et activités existants autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.3.3 :

- les extensions et les travaux sur les constructions à usage d'activité et les aménagements de leur terrain sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité ;
- les travaux sur les ouvrages de protection ;
- les travaux nécessaires au changement de destination de constructions existantes à usage d'activité à faible enjeu sous réserve de ne pas générer de présence humaine permanente ;
- les reconstructions en cas de sinistre, sans changement de destination.

Zones B1 et B2

Sont également admis :

- les extensions et les travaux sur les équipements techniques et les aménagements de leur terrain sous réserve de ne pas générer de présence humaine permanente ;
- les travaux sur les infrastructures ;
- les changements de destination de constructions sous réserve de ne pas augmenter le nombre de personnes exposées et de ne pas être destinés à l'habitation ou à un ERP ;
- les démolitions ;
- les travaux d'entretien des chemins de halage ;
- les travaux d'entretien et de stabilisation des berges des darses ;
- les travaux des espaces libres (plantations, dépollution, clôtures...) sous réserve de ne pas les ouvrir au public et de ne pas générer de présence humaine permanente.

II.3.3 - Prescriptions constructives

Les projets situés en zone B1 doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets de surpression et des effets thermiques continus et transitoires dont l'intensité est donnée en annexe du présent règlement.

Les projets situés en zone B2 doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets de surpression dont l'intensité est donnée en annexe du présent règlement.

Ces caractéristiques sont définies par une étude préalable[3] à la charge du maître d'ouvrage.

Font exceptions à cette obligation les extensions de bâtiments d'activité dont la surface de plancher est inférieure à 40 m² et ne nécessitant pas une présence humaine permanente.

Les effets thermiques continus et transitoires impactant les zones B1 et B2 peuvent faire l'objet de recommandations définies dans le cahier des recommandations joint.

3 Conformément à l'article *R.431.16.c) du code de l'urbanisme, la demande de permis de construire comporte une attestation certifiant la réalisation de cette étude et constatant que le projet prend en compte ces conditions au stade de la conception.

II.4 - Dispositions applicables en zones b1 et b2

On rappelle que les termes utilisés dans le paragraphe II.4 sont définis au titre II page 6.

II.4.1 - Dispositions applicables aux projets nouveaux

Article 13 - Projets nouveaux interdits

Hormis les projets autorisés à l'article 14, tous les projets nouveaux sont interdits.

Article 14 - Projets nouveaux autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.4.3 :

- les constructions à usage d'activité et les aménagements de leur terrain ;
- Les ERP non difficilement évacuables de catégorie 5, dans la limite de 20 personnes, en lien avec une activité existante dans la zone ;
- la réalisation d'ouvrages de protection :
  - ✗ des constructions ;
  - ✗ des infrastructures ;
  - ✗ des équipements techniques.
- La construction d'annexes de bâtiments d'habitation de gardiennage.

Sont également admis :

- les constructions d'équipements techniques sous réserve de ne pas générer de présence humaine permanente ;
- la réalisation d'infrastructures ;
- les aires de stationnement liés aux activités autorisées et celles nécessaires aux services publics ou d'intérêts collectifs.

II.4.2 - Dispositions applicables aux projets sur les biens et activités existants

Article 15 – Projets sur les biens et activités existants interdits

Hormis les projets autorisés à l'article 16, tous les projets sur les biens et activités existants sont interdits.

Article 16 – Projets sur les biens et activités existants autorisés

Sont admis sous réserve du respect des prescriptions constructives indiquées au II.4.3 :

- les extensions et les travaux des constructions d'habitation de gardiennage existantes et les aménagements de leur terrain, à l'exception des vérandas et des verrières, sous réserve :
  - ✗ de ne pas être un ERP ;
  - ✗ dans la limite de 20% de la surface de plancher existante ;
- les extensions et les travaux sur les constructions à usage d'activité et les aménagements de leur terrain ;

Zones b1 et b2

- les travaux nécessaires au changement de destination de constructions existantes à usage d'activité à faible enjeu sous réserve de ne pas générer de présence humaine permanente ;

- les travaux sur les ouvrages de protection ;

- les reconstructions en cas de sinistre ;

Sont également admis :

- les extensions et les travaux sur les équipements techniques et les aménagements de leur terrain sous réserve de ne pas générer de présence humaine permanente ;

- les travaux sur les infrastructures ;

- les changements de destination de constructions à usage d'activité sous réserve :
  - ✗ de ne pas être destinées à un ERP difficilement évacuable ;
  - ✗ de ne pas être un ERP de catégorie 1, 2, 3 ou 4 ;
  - ✗ de ne pas accueillir plus de 20 personnes.

- les démolitions ;

- les travaux d'entretien des chemins de halage ;

- les travaux d'entretien et de stabilisation des berges et des darses ;

- les travaux des espaces libres (plantations, dépollution, clôtures...).

II.4.3 - Prescriptions constructives

Les projets situés en zone b1 doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets de surpression et des effets thermiques transitoires dont l'intensité est donnée en annexe du présent règlement.

Les projets situés en zone b2 doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets de surpression dont l'intensité est donnée en annexe du présent règlement.

Ces caractéristiques sont définies par une étude préalable[4] à la charge du maître d'ouvrage.

Font exceptions à cette obligation :

- les extensions de bâtiments d'activité dont la surface de plancher est inférieure à 40 m² et ne nécessitant pas une présence humaine permanente ;

- la construction d'annexes de bâtiments d'habitation de gardiennage existants (abris de jardin, garage, ...), dont la surface de plancher est inférieure à 40 m² et non munie de vitrages.

Les effets de surpression et les effets thermiques transitoires impactant les zones b1 et b2 peuvent faire l'objet de recommandations définies dans le cahier des recommandations joint.

4 Conformément à l'article *R 431.16.c) du code de l'urbanisme, la demande de permis de construire comporte une attestation certifiant la réalisation de cette étude et constatant que le projet prend en compte ces conditions au stade de la conception.

II.5 - Dispositions applicables en zone G

On rappelle que les termes utilisés dans le paragraphe II.5 sont définis au titre II page 6.

II.5.1 - Dispositions applicables aux projets nouveaux

Article 17 – Projets nouveaux interdits

Hormis les projets autorisés à l'article 18, tous les projets nouveaux sont interdits.

Article 18 – Projets nouveaux autorisés

Sont admis sous réserve du respect de prescriptions constructives indiquées au II.5.3 :

- les constructions à usage d'activité et les aménagements de leur terrain, directement en lien avec l'activité à l'origine du risque sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité et de ne pas accueillir de public ;

- la réalisation d'ouvrages de protection :
  - ✗ des constructions ;
  - ✗ des infrastructures ;
  - ✗ des équipements techniques.

Sont également admis :

- les équipements techniques de services publics (ouvrages de distribution d'énergie, de produits pétroliers, d'alimentation d'eau potable, d'assainissement, de télécommunication...) sous réserve de ne pas générer de présence humaine permanente ;

- la réalisation d'infrastructures strictement nécessaires aux secours ou à l'activité à l'origine du risque ou au fonctionnement des services d'intérêt général.

II.5.2 - Dispositions applicables aux projets sur les biens et activités existants

Article 19 - Projets sur les biens et activités existants interdits

Hormis les projets autorisés à l'article 20, tous les projets sur les biens et activités existants sont interdits.

Article 20 - Projets sur les biens et activités existants autorisés

Sont admis sous réserve du respect des conditions d'utilisation et d'exploitation indiquées au II.5.3 :

- les extensions et les travaux des constructions à usage d'activité et les aménagements de leur terrain, directement en lien avec l'activité à l'origine du risque sous réserve d'accueillir une présence humaine strictement nécessaire à l'activité ;

- les travaux sur les ouvrages de protection ;

- les reconstructions en cas de sinistre.

Zone G

Sont également admis :

- les extensions et les travaux sur les équipements techniques et les aménagements de leur terrain sous réserve de ne pas générer de présence humaine permanente ;

- les travaux sur les infrastructures ;

- les changements de destination de constructions existantes sous réserve de ne pas augmenter le nombre de personnes exposées et de ne pas être destinés à l'habitation ou à un ERP ;

- les démolitions.

II.5.3 - Conditions d'utilisation et d'exploitation

Les interdictions, conditions et prescriptions particulières d'utilisation ou d'exploitation des sites sont fixées dans l'arrêté préfectoral d'autorisation au titre de la législation des installations classées des Établissements SOGEPP et TRAPIL.

Titre III - Mesures foncières

Sans objet.

Titre IV - Mesures de protection des populations

Les mesures imposées dans le présent Titre IV présentent un caractère obligatoire lorsque leur coût est inférieur à 10 % de la valeur vénale ou estimée du bien existant concerné à la date de prescription du PPRT conformément à l'article R.515-42 du code de l'environnement.

Si pour un bien donné, le coût des mesures dépasse 10 % de sa valeur vénale, les dispositions réalisables à hauteur de 10 % de cette valeur vénale sont mises en œuvre afin de protéger les occupants du bâtiment avec une efficacité aussi proche que possible des objectifs cités. Dans ce cas, se reporter au « Cahier des recommandations » du présent PPRT.

IV.1 - Mesures sur les constructions existantes

IV.1.1 - Mesures sur les constructions existantes en zone R

En zone R, les constructions existantes devront être compatibles à un usage d'activité sans présence humaine permanente dans un **délai de 5 ans** à compter de la date d'approbation du PPRT.

IV.1.2 - Mesures sur les constructions existantes en zone r

En zone r, les constructions existantes devront être compatibles à un usage d'activité sans présence humaine permanente dans un **délai de 5 ans** à compter de la date d'approbation du PPRT.

IV.1.3 - Mesures sur les constructions existantes en zone B1

En zone B1, les constructions existantes pouvant abriter des personnes doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets thermiques continus et transitoires dont l'intensité est donnée en annexe du présent règlement.

Ces mesures à la charge des propriétaires doivent être réalisées dans un **délai de 5 ans** à compter de la date d'approbation du PPRT.

IV.1.4 - Mesures sur les constructions existantes en zone B2

En zone B2, les constructions existantes pouvant abriter des personnes doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets de surpression dont l'intensité est donnée en annexe du présent règlement.

Ces mesures à la charge des propriétaires doivent être réalisées dans un **délai de 5 ans** à compter de la date d'approbation du PPRT.

IV.1.5 - Mesures sur les constructions existantes en zone b1

En zone b1, les constructions existantes pouvant abriter des personnes doivent présenter des caractéristiques de nature à garantir la protection des personnes pour des effets thermiques transitoires dont l'intensité est donnée en annexe du présent règlement.

Ces mesures à la charge des propriétaires doivent être réalisées dans un **délai de 5 ans** à compter de la date d'approbation du PPRT.

IV.2 - Mesures relatives aux usages

IV.2.1 - Transports collectifs sur route

Il est interdit d'implanter de nouveaux arrêts de bus dans le périmètre d'exposition aux risques.

Il est interdit d'implanter de nouvelles lignes de transports collectifs dans les zones R, r, B1 et B2.

Tous les transports collectifs respecteront strictement les arrêts déjà implantés dans le périmètre d'exposition aux risques.

IV.2.2 - Transports ferroviaires

Tout arrêt en zone rouge R est interdit à l'exception des dessertes d'entreprises.

IV.2.3 - Transports fluviaux

Tout stationnement le long du rivage, même temporairement, dans le périmètre d'exposition aux risques à l'exception de celui nécessaire à l'activité à l'origine du risque et aux activités liées à la voie d'eau (hors sports et loisirs) est interdit.

IV.2.4 - Espaces ouverts

Une signalisation d'information de l'existence d'un risque technologique, de type « zone à risques », à destination des usagers, est mise en place, dans un **délai d'un an** à compter de la date d'approbation du PPRT, par le propriétaire ou gestionnaire de l'espace, au niveau des entrées, dans le périmètre d'exposition aux risques.

La signalisation comprend une mention relative à l'attitude à adopter, par les usagers, en cas d'alerte.

IV.2.5 - Autres usages

De manière générale, tout stationnement susceptible d'augmenter, même temporairement, l'exposition des personnes est interdit (caravanes, résidences mobiles ou bâtiments modulaires dont l'occupation est permanente ou temporaire...) à l'exception du stationnement des véhicules nécessaire aux riverains ou aux activités locales et des bâtiments modulaires de chantier.

IV.3 - Mesures d'accompagnement

Les mesures d'accompagnement prévues par le PPRT concernent l'information sur les risques technologiques.

L'information du public se traduira par une signalisation d'information de l'existence d'un risque technologique, de type « zone à risques », qui sera mise en place, dans un **délai d'un an** à compter de la date d'approbation du PPRT, par le port de Paris :

- sur les rues « route du bassin n°6 », « route du bassin n°5 » et « chemin des petits marais » au niveau de leurs entrées dans le périmètre d'exposition aux risques ;
- sur la piste cyclable au niveau de ses entrées dans le périmètre d'exposition aux risques ;
- aux deux arrêts de bus existant dans le périmètre d'exposition aux risques (cartographiés à la page 29 de la note de présentation) ;
- dans l'avis à la batellerie n°1.

La signalisation comprend une mention relative à l'attitude à adopter, par les usagers, en cas d'alerte.

L'information est rendue obligatoire dans tous les ERP et activités industrielles et commerciales présentes à l'intérieur du périmètre d'exposition aux risques :

- l'affichage du risque et les consignes de sécurité en cas d'accident industriel ;

- une information annuelle des personnels, salariés et occupants permanents sur le risque existant et la conduite à tenir en cas de crise. La forme que prendra cette information (plaquette, réunion...) est laissée à l'appréciation du responsable de chaque établissement situé dans le périmètre d'exposition aux risques.

Conformément aux dispositions de l'article 8 du décret n° 2005-1156 du 13 septembre 2005 relatif au Plan Communal de Sauvegarde (PCS), la commune de Gennevilliers doit être couverte par un PCS.

Titre V - Servitudes d'utilité publique

Il s'agit des mesures instituées en application de l'article L.515-8 du code de l'environnement et des servitudes instaurées par les articles L.5111-1 à L.5111-7 du code de la défense.

Il n'a pas été instauré de servitudes d'utilité publique dans le cadre de ce PPRT.

ANNEXE : Dispositions constructives applicables aux constructions nouvelles et aux aménagements du bâti existant

Niveaux de protection à respecter

L'onde de surpression de référence et le flux thermique de référence à respecter sont extraits respectivement des cartographies des effets de surpression, des effets thermiques continus et transitoires ci dessous :

- carte « Enveloppes des intensités des effets de surpression à cinétique rapide » ;
- carte « Enveloppes des intensités des effets thermiques continus à cinétique rapide » ;
- carte « Enveloppes des intensités des effets thermiques transitoires à cinétique rapide ».

Groupe Qualiconsult

Renaud D'ACREMONT <renaud.dacremont@qualiconsult.fr>

Base Logistique - Greendock - Port de Gennevilliers 92

DUBRULLE Eric PP DSPAP DTSP92 <eric.dubrulle@interieur.gouv.fr> 28 septembre 2023 à 16:12
À : Renaud d'ACREMONT <renaud.dacremont@qualiconsult.fr>

Bonjour
actuellement il existe un CSU spécifique au port autonome de Paris. Ils ont un vidéo opérateur h24 au niveau de la capitainerie.
Le projet de déport d'image au CSU du commissariat vient d'être validé par la préfecture. Je ne connais pas le délai de mise en place technique, mais le projet étant déjà ancien, normalement le raccordement
devrait être rapide. (pour Gennevilliers nous avons un système dérogatoire avec le CSU installé au commissariat et non à la ville - de ce fait nous sommes aussi raccordés au PZVP - la vidéo de paris).
Cordialement

logo **Eric DUBRULLE**
Commandant Divisionnaire fonctionnel

adjoint au chef de service
CSPAP Gennevilliers
DTSP 92
Préfecture de Police
Tél. : 01 40 85 59 27

www.prefecturedepolice.paris

facebook

-------- Message original --------
Sujet : [INTERNET] Fwd: Base Logistique - Greendock - Port de Gennevilliers 92
De : Renaud d'ACREMONT <renaud.dacremont@qualiconsult.fr>
Pour : eric.dubrulle@interieur.gouv.fr
Date : 28/09/2023 10:19
[Texte des messages précédents masqué]

PRÉFECTURE
DE POLICE
Liberté
Égalité
Fraternité

Direction des Transports et de la Protection du Public
Service Opérationnel de Prévention Situationnelle

Paris, le 21 septembre 2023

Demande de compléments d'informations
Base Logistique Greendock – Gennevilliers (92).

à l'attention du cabinet Qualiconsult

Des éléments complémentaires doivent être précisés dans l' ESP.

P71 - « vidéo urbaine » – l'extrait de 2016 est-il vraiment pertinent ? Par ailleurs, s'agit-il de La Courneuve ou Gennevilliers ? Il serait judicieux de mentionner l'implantation du système de vidéoprotection urbaine et du report des images au commissariat de police nationale.

Qualiconsult :
L'extrait de 2016 a été supprimé.

Il s'agit de Gennevilliers, I Courneuve était une erreur. Pour la vidéo ville, nous avons pris contact avec le commandant DUBRULLE, qui donne les éléments ci-dessous.

Réponse à la demande par mail :

« Bonjour
actuellement il existe un CSU spécifique au port autonome de Paris. Ils ont un vidéo opérateur h24 au niveau de la capitainerie.
Le projet de déport d'image au CSU du commissariat vient d'être validé par la préfecture. Je ne connais pas le délai de mise en place technique, mais le projet étant déjà ancien, normalement le raccordement devrait être rapide. (pour Gennevilliers nous avons un système dérogatoire avec le CSU installé au commissariat et non à la ville - de ce fait nous sommes aussi raccordés au PZVP - la vidéo de paris).
Cordialement »

P76 – 7.1 – qu'en est-il du rapport de physionomie de la société privée mentionnée ? Concernant le trafic de stupéfiants, le paragraphe se rapporte-t-il au site concerné (proximité nouvelle gare) ?

Qualiconsult :

+ **Rapport de physionomie : Supprimé, cela fait référence à un retour de EUROPA PORT, gestionnaire du port.**
+ **Trafic de stupéfiants / nouvelle gare : La gare de proximité est sur la future ligne 15 (grésillon), prit en compte. Effectivement au vu de la distance, il y a une faible probabilité cependant je pense qu'une partie des salariés vont utiliser des transports en communs.**

P77 – 7.3 – intrusion attentat – quel est le chiffrage retenu concernant « le nombre important de personnes » ? effectif maximum sur site réponse MO

réorganisez les items contenus dans votre analyse de risques par groupes (atteintes aux biens, atteintes aux personnes) ; ex : « agression viol » à positionner dans les atteintes aux personnes.

Qualiconsult :

Fait.

Ci-dessous la réponse de la Maître d'Ouvrage par rapport aux précisions sur « le nombre important de personnes ».

Total des effectifs (équipe logistique + équipe bureaux) cumulé avec chevauchement de shift dans l'ensemble des cellules : 704 personnes.

P80 – mesures relatives au chantier – contradictions entre les pages 80 et 81 « mesures retenues », « prescriptions », « recommandations ». Clarifiez ces paragraphes. Par ailleurs, pensez-vous qu'une clôture posée autrement que verticalement peut être envisagée ??? (P82)

Qualiconsult :

Fait

P83 – la durée légale maximale d'enregistrement des images de vidéoprotection est de 30 jours.

Qualiconsult :

Oui. Corrigé à 30j.

P86 – reprendre la rédaction du paragraphe relatif à la circulation des forces de l'ordre.

Qualiconsult :

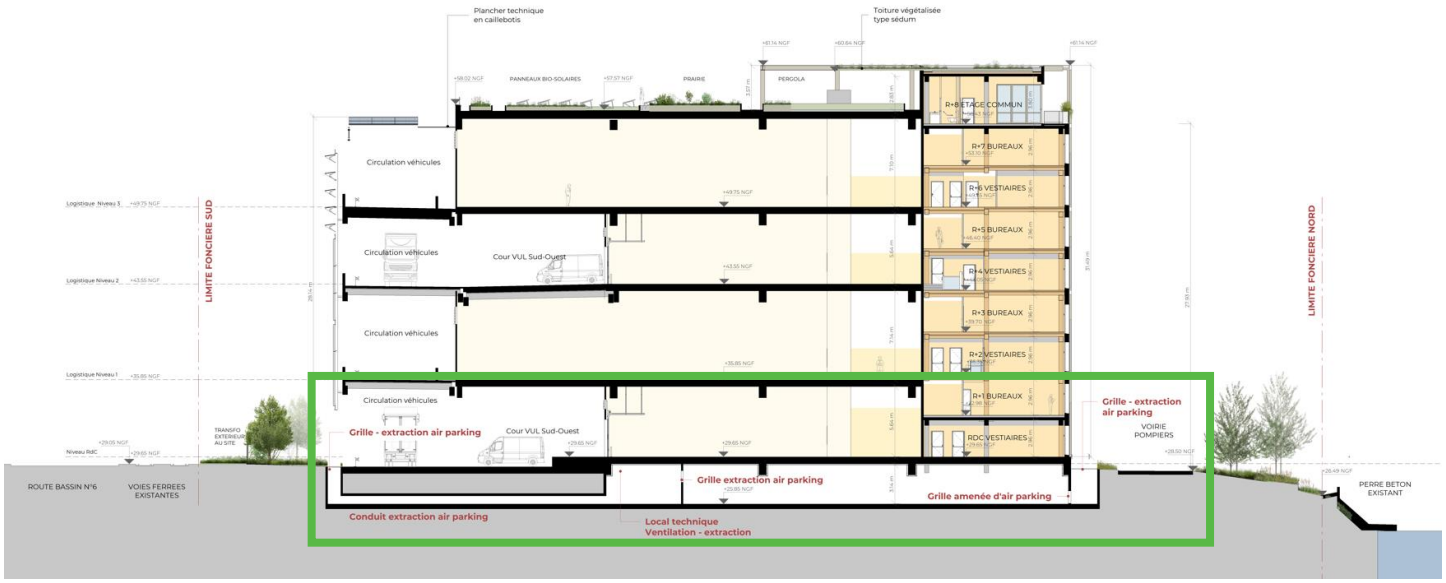
Fait

P94 – précisez la localisation des prises d'air neuf alimentant les niveaux de parking (SS1). Bien que les toitures soient classées en code du travail, précisez la hauteur et les caractéristiques des garde-corps.

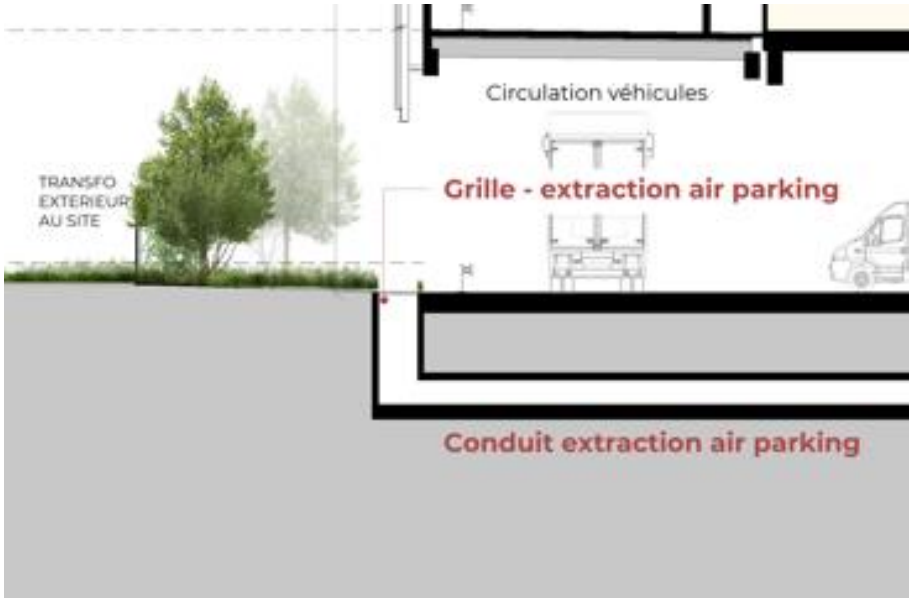
Qualiconsult :

Ci-dessous (et vous le trouverez aussi en annexe de l'ESP) les plans projets qui récapitulent :

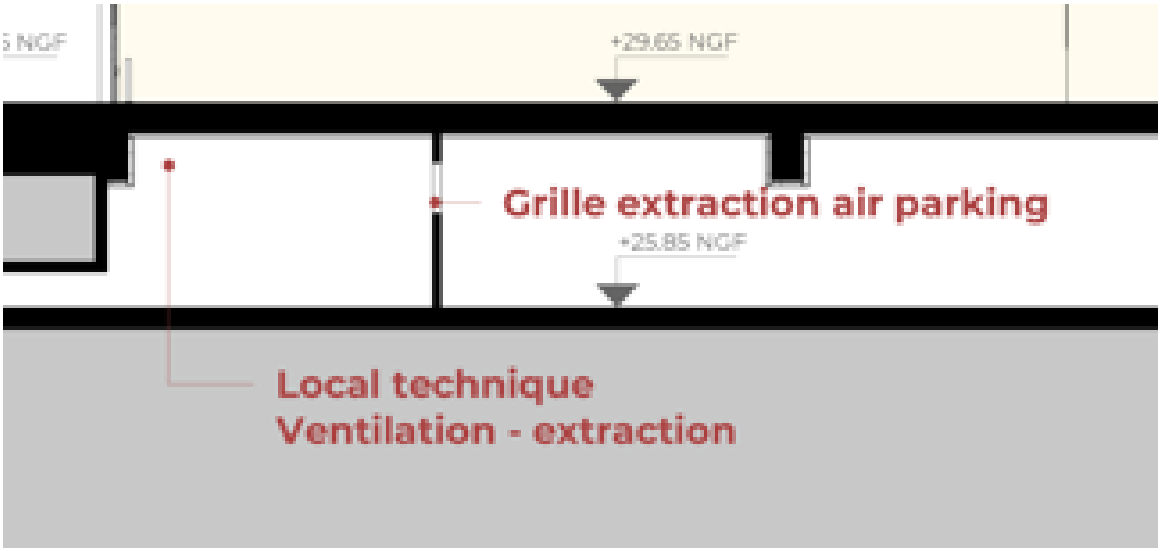
i. Les prises d'air au niveau du parking en sous-sol :



- Détail extraction d'air (côté sud)



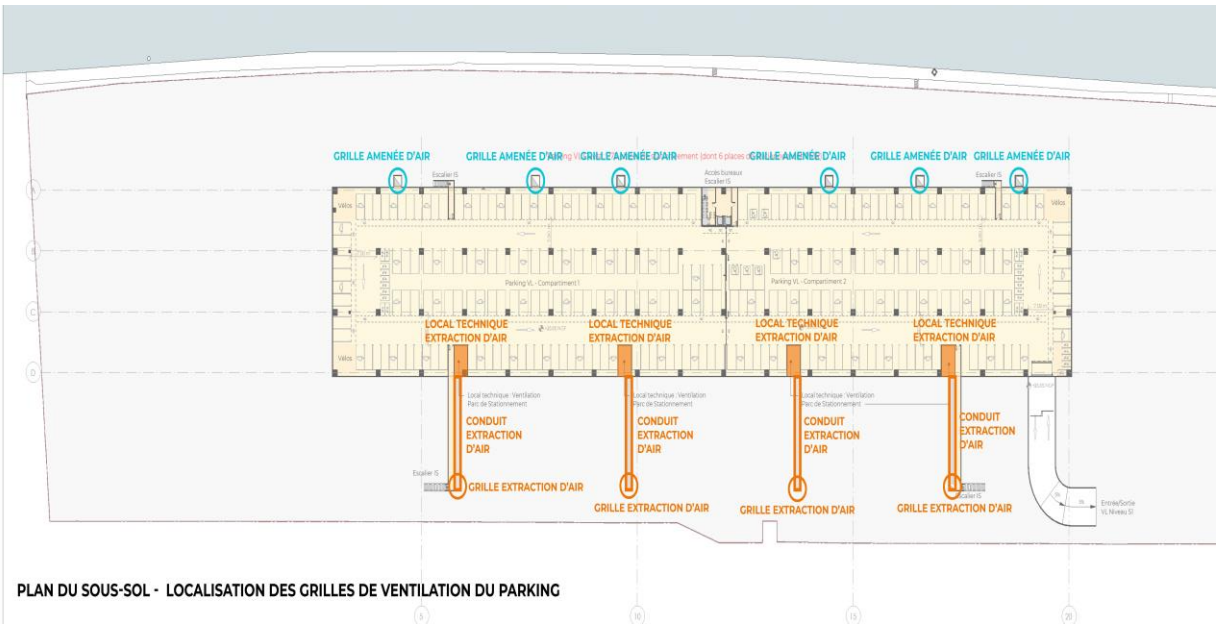
- Extraction air (central)



- Amenée d'air (nord)

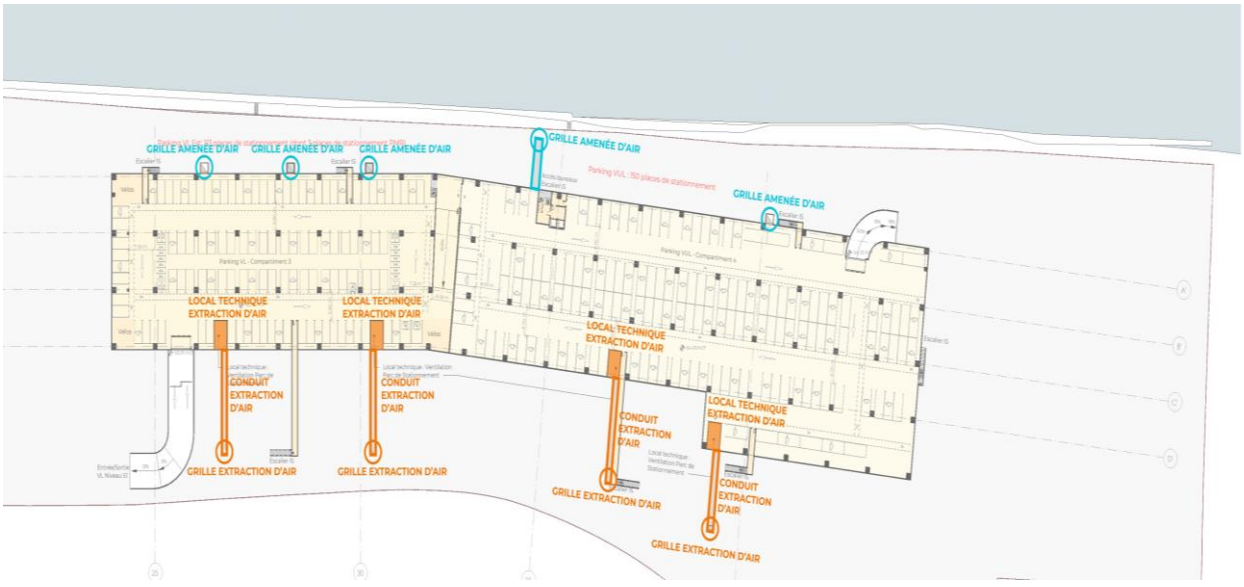

R+1 BUREAUX
+32.98 NGF
2.96 m
5.64 m
RDC VESTIAIRES
+29.65 NGF
2.96 m
3.14 m
Grille - extraction
air parking
VOIRIE
POMPIERS
+28.50 NGF
Grille amenée d'air parking

- Localisation des grilles de ventilation du parking

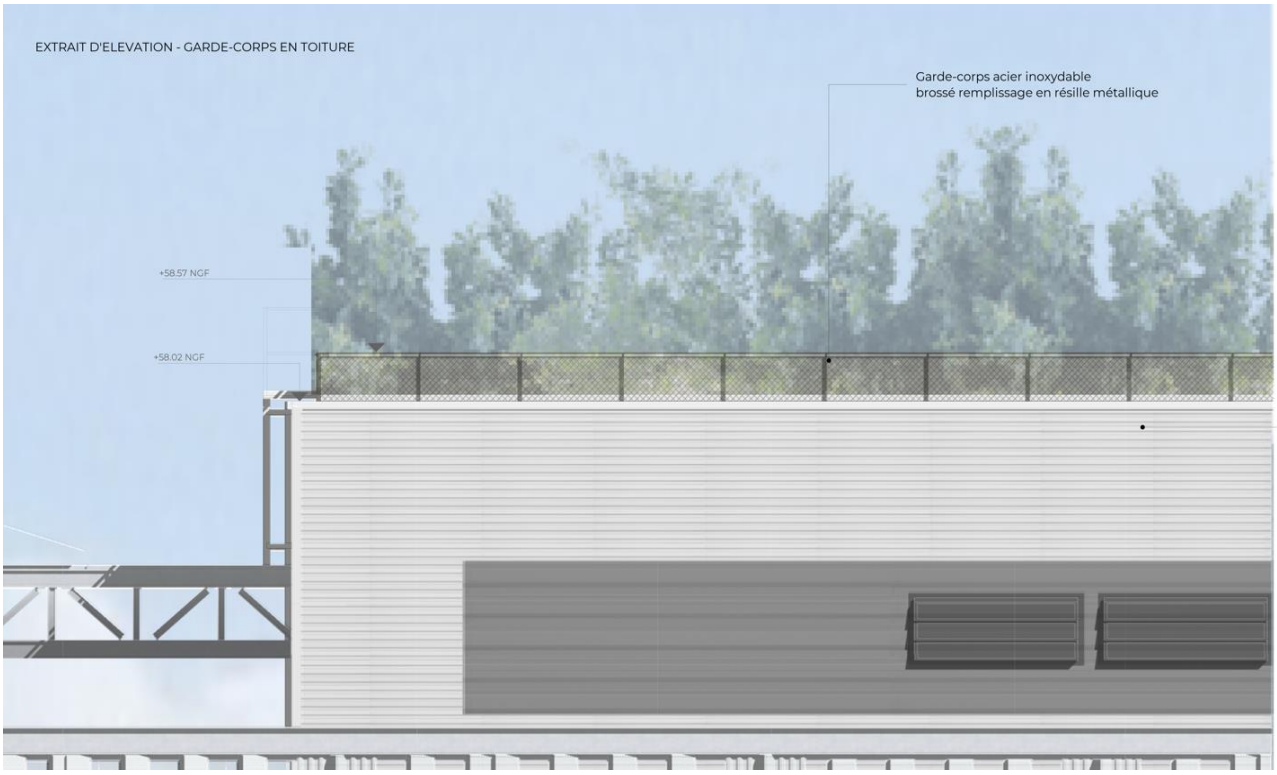


PLAN DU SOUS-SOL - LOCALISATION DES GRILLES DE VENTILATION DU PARKING

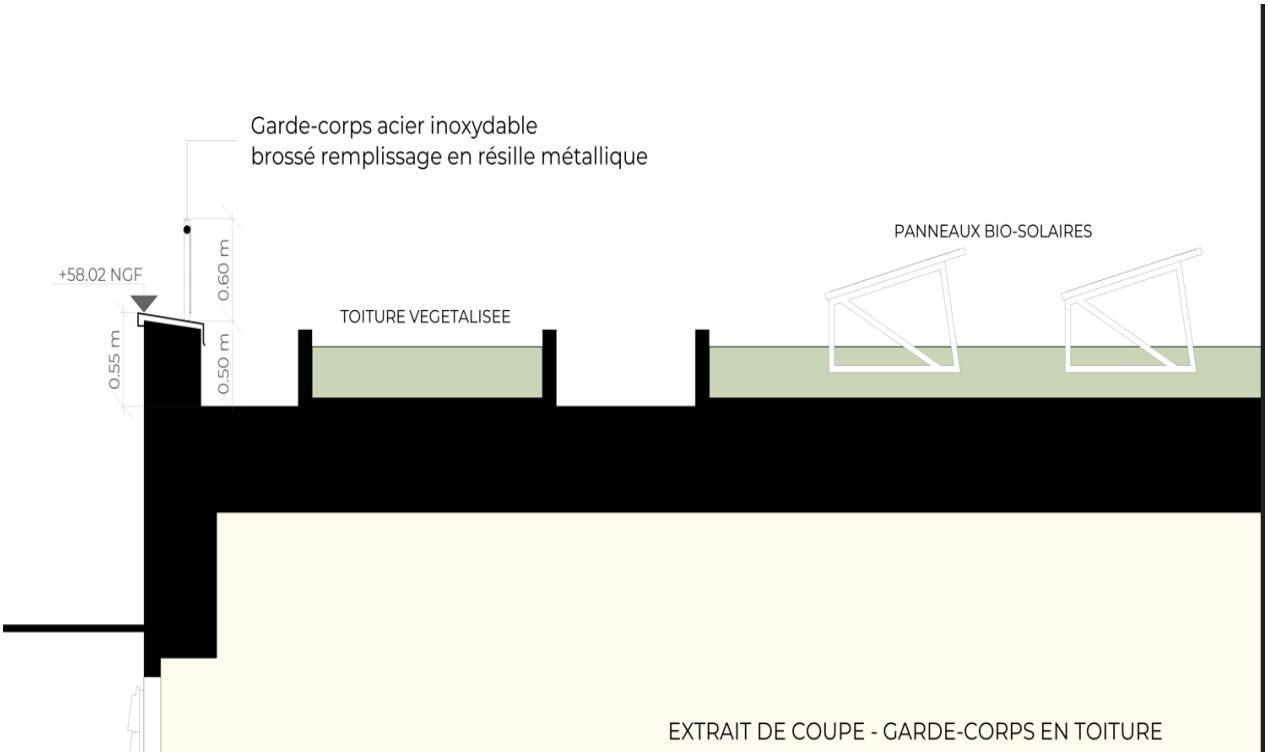
–



ii. Garde-corps en toiture



Garde-corps en toiture



Garde-corps en toiture terrasse

Mesure retenue par le projet

Les garde-corps périmétriques en toiture terrasse sont composés d'un acrotère de 50cm, surmonté d'un garde-corps en acier. Remplissage de la partie en garde-corps acier avec une résille métallique.

P96 – le schéma relatif au fonctionnement des barges est présent en double ; le retirer de la page 96.

Qualiconsult :
Fait

P98 – le plan des espaces intérieurs n'est pas lisible.

Qualiconsult :

Plans en annexe

P100 – rédigez un paragraphe sur le système de contrôle d'accès du site.

Qualiconsult :

Le site est totalement hermétique. Les différents accès sont contrôlés par des dispositifs de fermeture et une présence humaine. Les accès sont dédiés selon la finalité. Un accès est prévu pour chaque typologie d'usage (livraisons /enlèvement de marchandises, employés, visiteur.

P103 – reprendre « gardien 24h/7jours par semaine » : en permanence, 7 j/7, 24 h/24. **Fait** Reprendre également la rédaction de la phrase suivante : « *Bouton d'alerte relié aux parties administratives (gestionnaire), société de télésurveillance, et PC du port (attentat, intrusion, etc.)* ». Un report est-il effectué vers une société de télésurveillance en plus du PC ?

Qualiconsult :

Textes repris.

Bouton d'alerte relié aux parties administratives (gestionnaire), société de télésurveillance, et PC du port (attentat, intrusion, etc.) en doublon le bureau de la direction est également équipé d'un bouton d'alerte attentat ayant les mêmes fonctions ;

Le paragraphe suivant est relatif aux dispositions de contrôle d'accès ; le replacer dans la partie idoine.

Qualiconsult :

Fait

S'assurer des caractéristiques du bloc-porte du PC ; si effectivement il est classé en BP3, une serrure mettant en œuvre un temps de résistance équivalent doit être installé (A2P***).

Qualiconsult :

CR4 selon la norme EN 1627-1630 et équipée d'un visiophone

P104 - « *La société de télésurveillance prenant le relais en période de fermeture, fait la levée de doute depuis les caméras du site* » – Vous mentionnez dans les paragraphes précédents que le site fonctionne en permanence (24h24), de ce fait, une contradiction émerge. Qu'en-est-il ?

Qualiconsult :

Oui, le site fonctionne en 24/24

- **En cas de faits avérés et déclenchement d'une alerte, la société de télésurveillance peut à distance visionner le site avec les caméras et alerter les forces de l'ordre.**

P105 - « *Les portes sont de Classe de résistance CR3 selon la norme A2P (temps de résistance 5 mn)* ». La classe de résistance CR3 s'établit selon la norme EN NF 1627-1630 ; A2P est une certification.

Qualiconsult :

Correctif apporté et rappel sur les normes EN NF 1627-1630 au chapitre portes et serrures

P105 – contradiction dans le paragraphe : « ***Mesure retenue*** **-** *Dans la zone administrative et bureau une recommandation sera faite aux exploitants de prévoir un système d'occultation (stores intérieurs ou cloisons opaques) ne permettant pas de voir dans les bureaux et salle depuis les circulations. »* Clarifiez ce point.

Qualiconsult :

Mesure retenue

Le cahier des charges preneur précise que dans la zone administrative et bureau il y a un système d'occultation (stores intérieurs ou cloisons opaques), ne permettant pas d'avoir une vue dans les bureaux et salles depuis les circulations.

Reprendre également le paragraphe suivant relatif aux « locaux sensibles » et « modulation sonore ».

P106 – reprendre le premier paragraphe relatif à la mise à l'abri des usagers ; identifier des locaux permettant la mise à l'abri des personnes (murs/visuels/point d'eau/trousse de secours/bouton molleté…).

Qualiconsult :

Mise en sécurité et confinement attentat

Mesures retenues et consignées

Les portes pouvant servir au confinement sont équipées de boutons moletés coté intérieur pour les bureaux et de barre anti paniques pour les portes donnant sur les locaux de préparations et stockages de marchandises. Il n'y a pas de communication visuelle depuis les zones de circulation, ou nu moyen d'occultation est en place.

Les parois des locaux de mise à l'abri sont de facture robuste.

Ce contrôle est fait sur les mêmes fréquences que la vérification de la vidéo pour toutes les zones permettant un confinement attentat intrusion. Il y a également un stock de bouteilles d'eau si aucun point d'eau n'est accessible dans ces espaces (péremption à contrôler sur le registre des vérifications).

Matériel d'urgence obligatoire par locaux dédiés au confinement :

1 radio à piles avec l'inscription des fréquences : France Inter + 1 radio locale conventionnée par le préfet du département ;

Des piles de rechange sont prévues

1 paire de ciseaux

1 lampe de poche avec des piles ou sur dynamo (ce dernier choix est préférable)

Plusieurs rouleaux de ruban adhésif large pour calfeutrer les aérations, grilles de ventilation, etc.

Eau en bouteilles si il n'y a pas de point accessibles dans la zone pour une hydratation régulière (date de péremption à contrôler régulièrement).

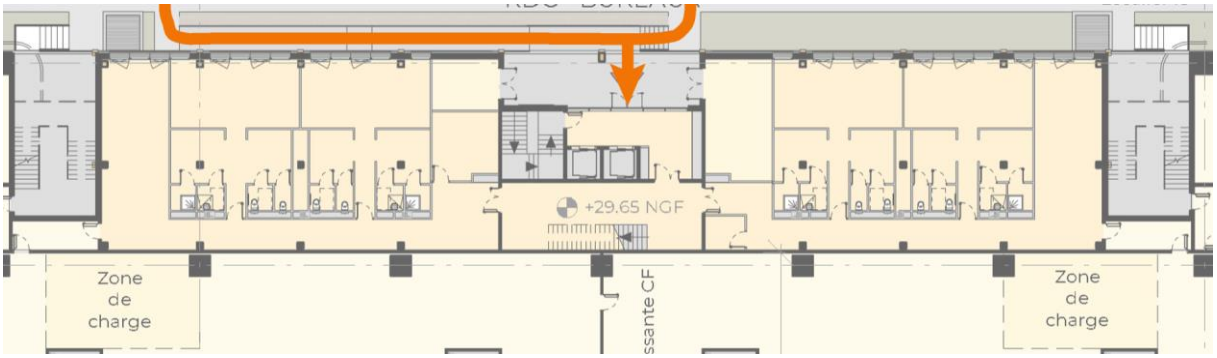
Une vérification périodique est consignée sur le registre sécurité sûreté à la charge du preneur.

Matériel d'urgence facultatif :

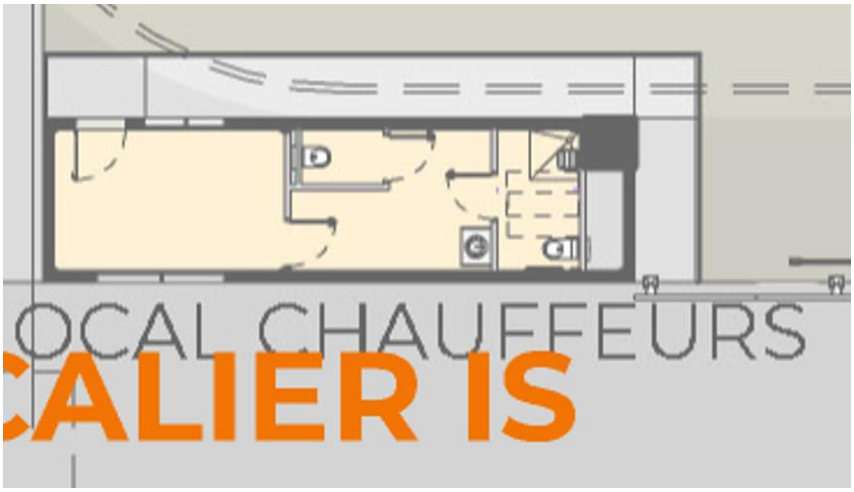
Essuie-tout, linges, chiffons, serpillières pour absorber d'éventuels liquides ou calfeutrer portes et fenêtres

1 seau ou des sacs en plastique en l'absence de WC

Prévoir des jeux de cartes, dés, papier, crayons, etc.



- Zone de confinement avec point d'eau et sanitaires, zone employés



- Zone de confinement pour les chauffeurs, local aveugle

- **Mesures retenues**
- **Les zones repérées et pouvant être utilisées au confinement sont actuellement envisagées dans les espaces sanitaires employés (un local par étage de cellule logistique) et local pause chauffeurs.**
- **Les locaux sanitaires à rez-de-chaussée sont équipés de châssis avec limiteur d'ouverture et stores d'occultation.**
- **Les chauffeurs peuvent également se réfugier dans les cabines des PL.**

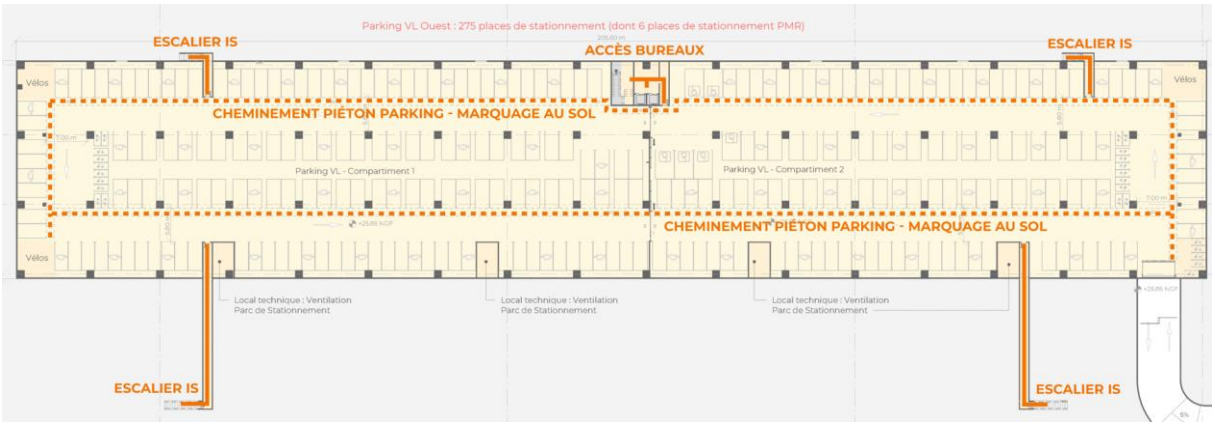
P107 – que vient faire le paragraphe suivant dans ce chapitre : « *L'objectif est de garantir la sécurité et le confort des circulations douces tout en assurant une fluidité de circulation. Une information régulière et efficace, tant des riverains que des usagers de la route sur la progression et la localisation des chantiers et les contraintes imposées par les travaux, sera effectuée » ?* Le placer dans les mesures relatives au chantier.

Qualiconsult :

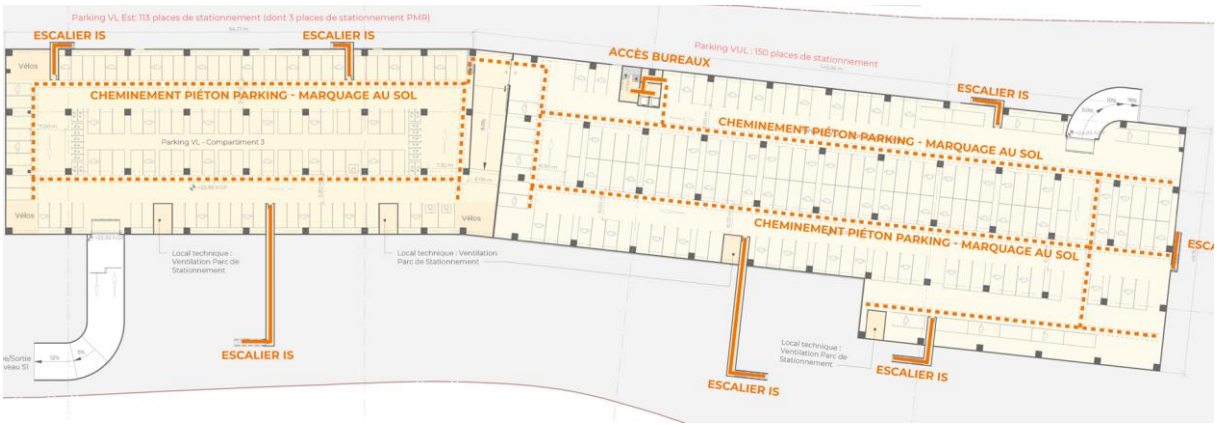
Fait

La partie relative aux espaces piétonniers n'est pas claire ; la reprendre ; par ailleurs, quels sont les dispositifs de protection des piétons et leur implantation ?

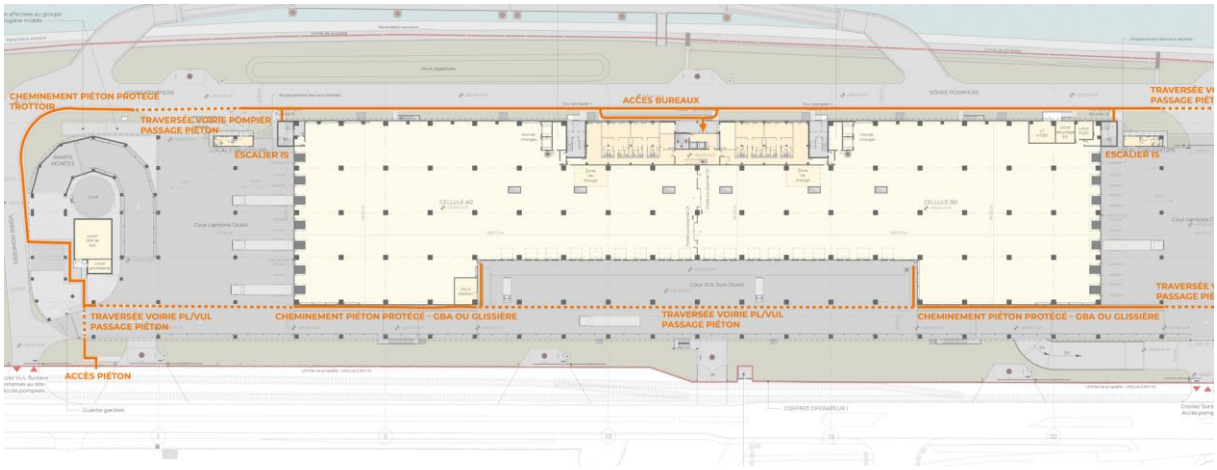
(Vous trouverez les plans exposés ci-dessous en annexe de l'ESP également)



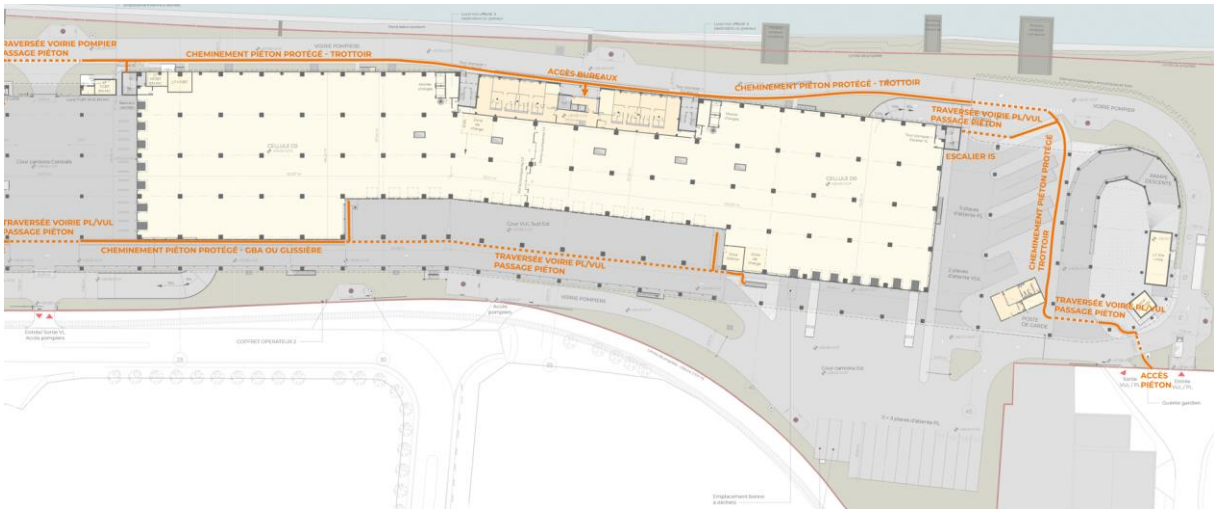
Circulation piétonne sous-sol aile Ouest



Circulation piétonne sous-sol aile Est

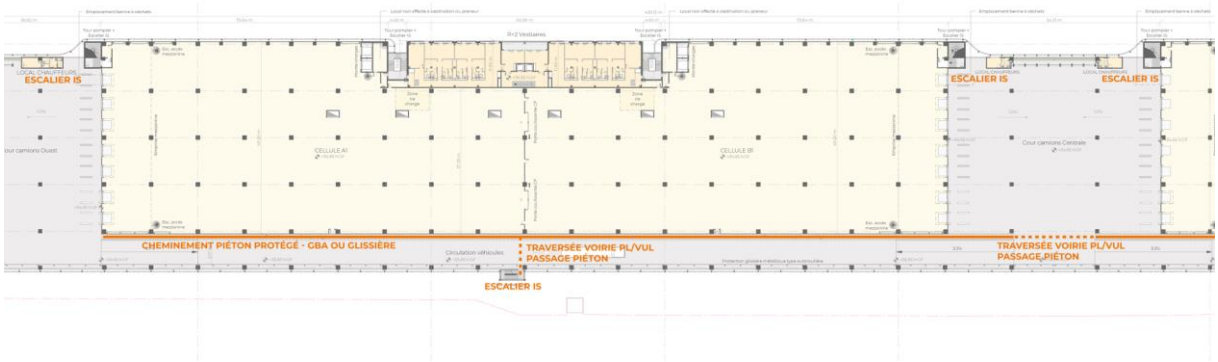


Circulation piétonne rez-de-chaussée aile Ouest



Circulation piétonne rez-de-chaussée aile Est

REPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité
PREFECTURE DE POLICE – 9, boulevard du Palais – 75195 PARIS CEDEX 04 – Tél. : 01 53 71 53 71 ou 01 53 73 53 73
Serveur vocal : 08 91 01 22 22 *(0,225 € la minute)*
http://www.prefecturedepolice.interieur.gouv.fr – mél : courriel.prefecturepoliceparis@interieur.gouv.fr

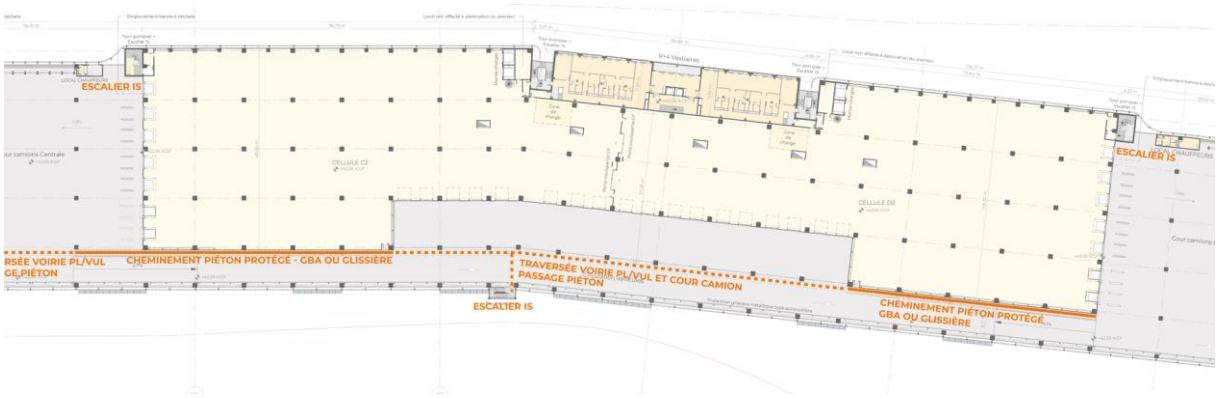


Circulation piétonne au R+1 aile Ouest

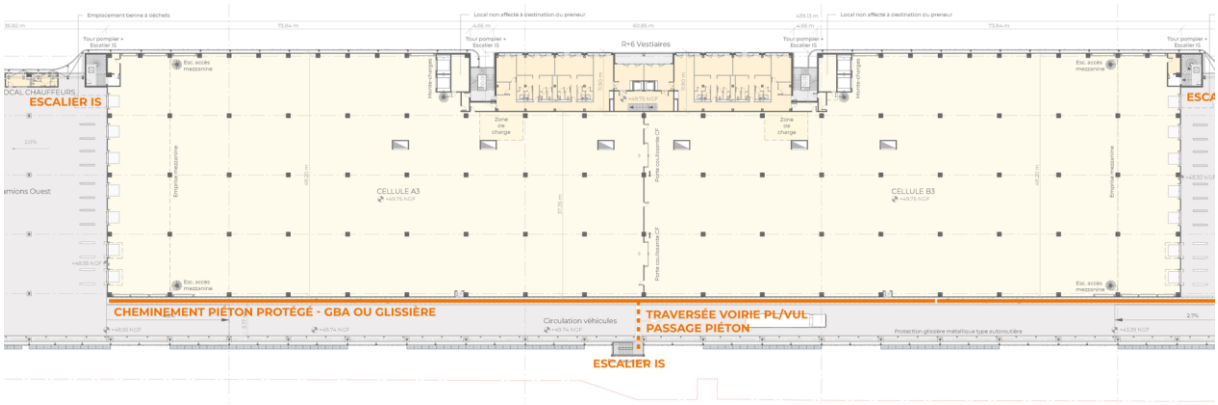
Circulation piétonne au R+1 aile Est

Circulation piétonne au R+2 aile Ouest

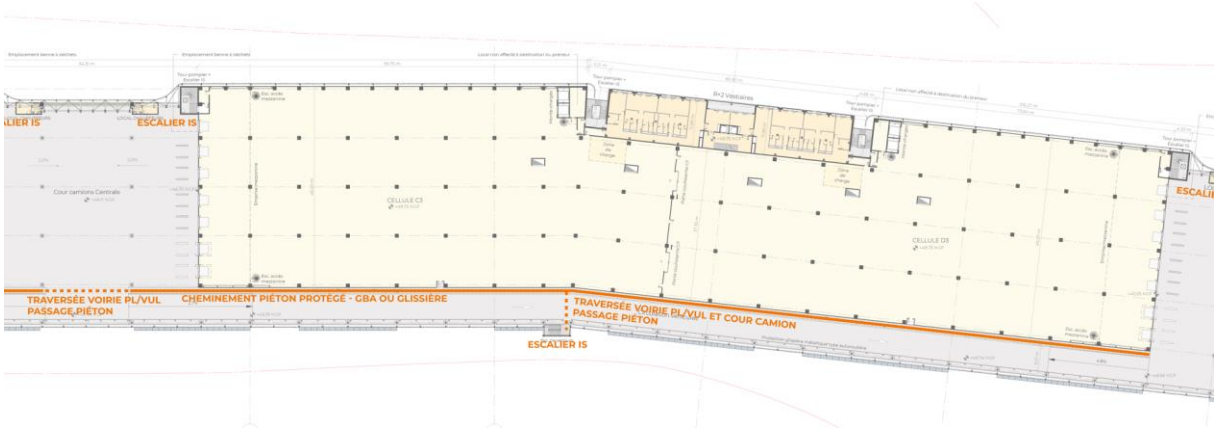
REPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité
PREFECTURE DE POLICE – 9, boulevard du Palais – 75195 PARIS CEDEX 04 – Tél. : 01 53 71 53 71 ou 01 53 73 53 73
Serveur vocal : 08 91 01 22 22 *(0,225 € la minute)*
http://www.prefecturedepolice.interieur.gouv.fr – mél : courriel.prefecturepoliceparis@interieur.gouv.fr



Circulation piétonne au R+2 aile Est



Circulation piétonne au R+3 aile Ouest



Circulation piétonne au R+3 aile Est

Mesure retenue :
Les cheminements piétons sont sécurisés contre les risques d'intrusion de véhicules (y compris deux roues) ;
La visibilité ainsi que la surveillance naturelle des cheminements piétons sont garanties ;
Les cheminements piétons sont éclairés.
Les zones à l'écart ou trop densément plantées ne sont pas prévues sur l'environnement du site ;
Cheminements avec marquage au sol ;
Passages piéton prévues à chaque étage pour connecter les zones extérieurs à l'intérieur du bâtiment;

Reprendre le tableau récapitulatif en tenant compte des modifications apportées suite à cette demande de renseignements.

Qualiconsult :

Fait

Ces éléments de réponses devront nous parvenir sous forme de questions/réponses ; ces éléments devront être annexés en fin de document lors du dépôt auprès des services instructeurs.

Le Service Opérationnel de Prévention Situationnelle